

CHILD PORNOGRAPHY ON THE INTERNET

Evaluating Preventive Measures
in order to Improve their Effectiveness in the EU Member States



DAPHNE 2000 - 2003

*With financial support from
the DAPHNE Programme*

European Commission

Edited by
Barbara Vettori

 **TRANSCRIME**

IN COOPERATION WITH:
UNICEF-INNOCENTI RESEARCH CENTRE
(FLORENCE, ITALY)

UNISYS BELGIUM SA
(BRUSSELS, BELGIUM)



UNIVERSITÀ DEGLI STUDI
DI TRENTO



UNIVERSITÀ CATTOLICA
DEL SACRO CUORE

CHILD PORNOGRAPHY ON THE INTERNET

EVALUATING PREVENTIVE MEASURES IN ORDER TO IMPROVE THEIR EFFECTIVENESS

IN THE EU MEMBER STATES

FINAL REPORT

EXECUTED BY

TRANSCRIME

IN COOPERATION WITH

UNICEF

INNOCENTI RESEARCH CENTRE

AND

UNISYS BELGIUM

FOR THE

EUROPEAN COMMISSION

WITH FINANCIAL SUPPORT FROM THE DAPHNE PROGRAMME

EUROPEAN COMMISSION (CONTRACT 01/097/C)

Università degli Studi di Trento

January 2007

Transcrime Reports n. 15

The content of this report represents the views of its authors and not necessarily those of the European Commission.

© 2007 Transcrime and European Commission

TABLE OF CONTENTS

1. FOREWORD	3
2. ACKNOWLEDGEMENTS	7
3. EXECUTIVE SUMMARY	11
4. AIM AND OBJECTIVES OF THE STUDY	29
5. OPERATIONAL DEFINITIONS	31
6. INTRODUCTION	33
7. FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION A (DETECTION AND CONTROL) BY TRANSCRIME	35
7.1 INTRODUCTION	35
7.2 METHODOLOGICAL STEPS	35
7.3 EU GUIDELINES AGAINST CHILD PORNOGRAPHY ON THE INTERNET AS REGARDS AREA OF INTERVENTION DETECTION AND CONTROL	39
7.4 EVALUATING THE LEVEL OF ADHERENCE OF EU MEMBER STATES LEGISLATION TO THE EU GUIDELINES	43
7.5 EVALUATING THE EFFECTIVENESS OF THE PREVENTIVE MEASURES IN PLACE IN EU MEMBER STATES AGAINST CHILD PORNOGRAPHY ON THE INTERNET	50
7.6 CONCLUSIONS.....	56
8. FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION B (SELF-REGULATION) BY TRANSCRIME	61
8.1 INTRODUCTION	61
8.2 METHODOLOGICAL STEPS	61
8.3 INTERNET SELF-REGULATION IN THE EUROPEAN UNION: AN OVERVIEW	63
A) SELF-REGULATION INITIATIVES DEVELOPED BY INTERNET SERVICE PROVIDER ASSOCIATIONS.....	67
8.4 EU GUIDELINES PERTAINING TO ISPAS IN RELATION TO CHILD PORNOGRAPHY ON THE INTERNET	67
8.5 MAPPING ISPAS CODES OF CONDUCT	69
8.6 EVALUATING THE LEVEL OF ADHERENCE TO EU GUIDELINES OF ISPAS CODES OF CONDUCT IN EU MEMBER STATES	72
8.7 EVALUATING THE EFFECTIVENESS OF CODES OF CONDUCT	74
B) SELF-REGULATION INITIATIVES DEVELOPED BY HOTLINES.....	80
8.9 EU GUIDELINES FOR NATIONAL INTERNET HOTLINES	80
8.10 MAPPING THE NATIONAL INTERNET HOTLINES IN EU MEMBER STATES	82
8.11 EVALUATING THE LEVEL OF ADHERENCE TO EU GUIDELINES OF THE SELF-REGULATION INITIATIVES DEVELOPED BY NATIONAL INTERNET HOTLINES IN EU MEMBER STATES	85
8.12 EVALUATING NATIONAL INTERNET HOTLINES IN EU MEMBER STATES	87
8.13 NATIONAL INTERNET HOTLINES	92
8.14 CONCLUSIONS.....	99

9. FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION C (AWARENESS AND EDUCATIONAL INITIATIVES) BY WORD & PICTURE LANGPORT AND UNICEF – INNOCENTI CENTRE FIRENZE	103
9.1 EVALUATING PREVENTIVE MEASURES IN ORDER TO IMPROVE THEIR EFFECTIVENESS IN THE EU MEMBER STATES, BY WORDS & PICTURES, LANGPORT	103
9.2 EVALUATING PREVENTIVE MEASURES IN ORDER TO IMPROVE THEIR EFFECTIVENESS IN THE EU MEMBER STATES, BY UNICEF INNOCENTI CENTRE, FIRENZE	110
10. FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION D (TECHNOLOGICAL MEASURES)	
BY UNISYS BELGIUM	151
10.1 INTRODUCTION	151
10.2 LIST OF ACRONYMS	153
10.3 CHILD PORNOGRAPHY ON THE INTERNET.....	154
10.4. PROTECTIVE TECHNICAL DEVICES	161
10.5. TRACEABILITY OF INTERNET ABUSERS	177
10.6 EVALUATION OF EFFECTIVENESS OF TECHNOLOGICAL MEASURES TO TACKLE CHILD PORNOGRAPHY ON THE INTERNET	188
10.7 CHOOSING THE RIGHT PROTECTIVE DEVICES.....	189
10.8 HOW TO USE THE INDICATORS: THE RESPECTIVE PROS AND CONS	204
10.9 INDICATOR RELEVANCE ACCORDING TO LOCATION OF CONTROL.....	210
10.10 OVERVIEW OF EXISTING PRODUCTS.....	212
10.11 CONCLUSION.....	217
11.RECOMMENDATIONS	219
12.BIBLIOGRAPHY	225
13. ANNEXES REGARDING AREA OF INTERVENTION A (DETECTION AND CONTROL):	237
14. ANNEXES REGARDING AREA OF INTERVENTION B (SELF-REGULATION):	279
15. ANNEXES REGARDING AREA OF INTERVENTION C (AWARENESS AND EDUCATIONAL FIELD)	309
16. ANNEXES REGARDING AREA OF INTERVENTION D (TECHNOLOGICAL MEASURES)	349

1. FOREWORD

This Final Report presents the results of the Study *Child Pornography on the Internet – Evaluating Preventive Measures in order to Improve their Effectiveness in the EU Member States*, funded by the EU Commission under the DAPHNE Programme 2000–2003 (Contract 01/097/c) and carried out by Transcrime, Joint Research Centre on Transnational Crime, Università degli Studi di Trento – Università Cattolica del Sacro Cuore di Milano, in cooperation with Unicef – Innocenti Research Centre, Firenze and Unisys Belgium.

The aim of the Study was to evaluate the effectiveness of the preventive measures in place in EU Member States, in the field of child pornography on the Internet in order to contribute to their improvement. To achieve this aim, the Study set itself the following objectives:

1. to map the preventive measures in place in EU Member States against child pornography on the Internet;
2. to assess (where possible) the level of adherence to EU guidelines of the preventive measures against child pornography in place in EU Member States;
3. to assess the effectiveness of the preventive measures against the child pornography on the Internet in place in EU Member States;
4. to identify good practices in the field of preventive measures against child pornography on the Internet in place in EU Member States and to disseminate them; to identify ways and forms to improve the effectiveness of such measures.¹

For the purposes of this Study, the term “child pornography” shall mean “pornographic material that visually depicts a child engaged in sexually explicit conduct”.² The concept of child pornography thus defined includes so-called ‘virtual child pornography’,³ that is pornographic material created either by manipulating existing pictures or by producing a combined image from different pictures, or even those that are entirely computer-generated.

The term “prevention” was defined as the set of all those measures, whose general goal is to “reduce the level of a crime”. For the purpose of this Study, “preventive measures” were therefore considered “those legislative, regulatory actions and technical devices whose goal (outcome) is to reduce the overall level of pornographic material circulating in Internet”. In the field of child pornography on

¹ The approved project originally set itself an additional objective, i.e. objective 5) to turn the findings of the evaluation into practical tools to be used by practitioners. After consultation with the partners and having decided during the seminar held in Bruxelles on 15 and 16 January 2004 that the state of art of the topic is still in its infancy, it was decided not to pursue it.

² Communication from the Commission to the Council and the European Parliament, “Combating trafficking of human beings and combating sexual exploitation of children and child pornography” – Proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography, COM (2000) 854 final/2.

³ *Manual on Child Pornography Legislation*, research done by Mrs. Conny Rijken assigned by Europol, Trafficking in Human Beings Unit, March 2001, pp. 9–10.

the Internet, prevention is the outcome that can be achieved through different interventions:

- *Area of Intervention A: Detection and Control:* the main actors in this area are the Law Enforcement Agencies of the EU Member States;
- *Area of Intervention B: Self-regulation:* the main actors in this field are National Internet Hotlines and Internet Service Providers as they play an important role as institutions directly involved in both the prevention and the removal of child pornography on the Internet;
- *Area of Intervention C: Awareness and Educational Initiatives:* The main actors in the field are governments, NGOs, educators and all the Institutions and bodies working on raising awareness about child pornography on the Internet;
- *Area of Intervention D: Technological Measures:* technology plays an important role in child pornography on the Internet. On one hand it is an instrument that is exploited by paedophiles to achieve their goals and on the other it is a powerful instrument for the prevention for their illegal activities.

Therefore, the activities undertaken to reach the aim and objectives of the Study were conducted in relation to each of the four above-mentioned Areas of intervention.

The Study was directed by Ernesto U. Savona, Professor of Criminology at the Università Cattolica del Sacro Cuore di Milano and Director of Transcrime.

A Steering Committee with the function of advising, suggesting, monitoring and following the development of the Study was appointed at its beginning. The following experts were part of the committee:

- Bjorn Clarberg, Europol, Serious Crime Department, Unit Crimes against Persons Unit, Group Trafficking in Human Beings;
- Jos Dumortier, Professor at the K. U. Lueven and Director of the ICRI (*Interdisciplinary Centrum voor Recht en Informatica*), Belgium;
- Japp E. Doek, Chairman of the UN Committee on the Rights of Children.

This Final Report complements an Intermediate Report delivered to the European in April 2003, and which included only the findings from objective 1 above. For the sake of completeness, the research findings of the Intermediate Report have been partially reproduced in this Final Report.

This Final Report has been edited by Barbara Vettori, Researcher in Criminology at the Università Cattolica del Sacro Cuore of Milan and Research Coordinator of Transcrime (Milan office).

The research and this Report are the result of the involvement of a variety of persons, institutions and activities. The responsibilities were divided as follows: Areas of intervention A and B were managed by Transcrime; Area of intervention C was managed by the Innocenti Research Centre – UNICEF; Area of intervention D was managed by UNISYS.

Transcrime managed Areas of intervention A (Detection/control measures) and B (Self-regulation), and wrote the related sections in this Final Report, as well as the related questionnaires, bibliography and synoptic tables.

UNICEF – Innocenti Research Centre managed Area of Intervention C (Awareness and education initiatives) and wrote the related sections in this Final Report, as well

as the related questionnaires, bibliography and synoptic tables. Mr. Cater, as Transcrime's consultant, edited the IRC Report.

UNISYS Belgium managed Area of Intervention D (Technological measures) and wrote the related sections in this Final Report, as well as the related annexes.

Transcrime conceptualised, organised and wrote all the remaining sections of this report, and inserted and collated the contributions from UNICEF and UNISYS.⁴

The Final Report is organised as follows:

- Chapter 1 is this Foreword;
- Chapter 2 includes the Acknowledgements;
- Chapter 3 is the Executive Summary of The Study;
- Chapter 4 specifies the aim and objectives of the Study;
- Chapter 5 provides the operational definitions of the key concepts of the Study;
- Chapter 6 is the introduction;
- Chapters 7 to 10 presents the findings from the Study, by each of the four different Areas of Intervention dealt with by the Study (the results for Area of Intervention A: Detection and Control are given in Chapter 7; the results for Area of Intervention B: Self-regulation are given in Chapter 8; the results for Area of Intervention C: Awareness and Educational Initiatives are given in Chapter 9; the results for Area of Intervention D: Technological Measures are given in Chapter 10;
- Chapter 11 contains the Recommendations addressed to the European Commission on the basis of the findings of the Study;
- Chapter 12 lists the Bibliography consulted for the Study.

This Report is complemented by four Annexes (Chapters 13 to 16).

The content of this report is the sole responsibility of its authors and, in no way, represents the views of the European Commission or its services.

⁴ In particular, Transcrime's responsibilities in the Reports were the following:

Barbara Vettori edited this Final Report and wrote chapters 1, 2 and 3.

Leonardo Dal Negro wrote chapters 4, 5, 6 and 11.

Regarding Section 1 (Area on intervention Detection and Control), Leonardo Dal Negro wrote paragraphs 7.1, 7.2, 7.5 and 7.6. Sabrina Adamoli wrote paragraph 7.4. She also drafted the questionnaire for the mapping activity (Chapter 13, Annex 1) and processed all the data gathered from the questionnaire.

Leonardo Dal Negro and Mara Mignone were responsible for drafting the questionnaire for the evaluation activity (Chapter 13, Annex 3). Leonardo Dal Negro processed all the data gathered through this questionnaire.

Regarding Section 2 (Area of intervention Self-regulation) Daria Angelini wrote paragraphs 8.4, 8.5, 8.6, 8.7 and 8.8 related to ISP self-regulation. She was also responsible for drafting the questionnaire for the evaluation activity regarding ISPs (Chapter 14, Annex 4). Shawna Gibson wrote paragraphs 8.9, 8.10, 8.11, 8.12 and 8.13 and 8.14 related to the Hotlines self-regulation. She was also responsible for the drafting of the questionnaire for the evaluation activity related to Hotline self-regulation (Chapter 14, Annex 2). Sabrina Adamoli developed the mapping activity of ISPs and Hotlines (Chapter 14, Annexes 1 and 3).

Nicholas Cater, from Words & Pictures, participated in the Study as a Transcrime expert in the field of Awareness and Educational Initiatives.

2.

ACKNOWLEDGEMENTS

We are indebted to Patric Trousson, DG JHA of the European Commission, who provided valuable help and support throughout the duration of the Study.

Special thanks go both to June Kane, consultant to the EU Commission, who has helped solving the problems connected with the management of the project and advised Transcrime on how better achieve its final goals, and to Richard Swetenham of the European Commission for his advice and input concerning various aspects of the project.

Different experts and institutions have contributed to this Report. They are listed according to the four areas of intervention analysed in the Project.

For *Area of Intervention A (Detection and control measures)*, Transcrime is grateful to the following experts, who responded to our questionnaires:

- A. Ahlenius, DI Child Protection Team, NCIS, Sweden;
- A. Andreakou, State Security Division, National Police, Greece;
- S. Ask, NICS, Sweden;
- R. Buchman, Federal Ministry of the Interior, Bundeskriminalamt;
- T. Dixon, National Bureau of Criminal Investigation, *Garda Siochana*, Ireland;
- T. Erents, Child Pornography Unit, National Police Agency, the Netherlands;
- V. Evangelos, National Police, Greece;
- C. Farinha and J. Duque, *Policia Judiciaria*, Portugal;
- M. Ford, NHTCU, United Kingdom;
- Y. Goethals, DGJ/DJP/MH Federal Police, Belgium;
- R. Gross, Federal Ministry of the Interior/Interpol, Austria;
- L. Henriksson, Criminal Intelligence Division, National Bureau of Investigation, Finland;
- D. Lowe, NHTCU, United Kingdom;
- S. Manke, *BundesKriminalamt Wiesbaden*, Germany;
- G. Manzi and L. Mancuso, *4th Investigative Section*, Carabinieri, Italy;
- C. Miche, Unit D.N.R.A.P.B., Judicial Police, France;
- J. Salom Clotet, Computer Crime Unit, *Guardia Civil*, Spain;
- S. Thomassen, Head of Cybercrime Unit, National Commimssioner Police;
- D. Toledo Artega, *Unidad de Investigacion Delinquencia Technologica Informatica*, Ministry of the Interior, Spain;
- L. Underbjerg and Mrs. B. Rønne, NCIS, Denmark;
- C. Weydert, *Police Grand-Ducale*, Luxembourg.

Special thanks go to Bjorn Clarberg, of the Trafficking in Human Beings Unit at Europol, for his precious cooperation in identifying contacts in specialised law

enforcement units in all EU Member States, and in distributing the questionnaires developed for the Study.

For *Area of Intervention B (Self-regulation)*, Transcrime gratefully acknowledges the cooperation of the following members of INHOPE, the Association of Internet Hotline Providers in Europe, who responded to our questionnaire:

- Stopleveline, Austria;
- Child Focus, Belgium;
- Red Barnet, Denmark;
- Save the Children, Finland;
- AFA, France;
- Electronic Commerce Forum, Germany;
- FSM, Germany;
- Jugendshutz, Germany;
- ISPAl, Ireland;
- Save the Children, Italy;
- Meldpunt, Netherlands;
- Protegeles, Spain;
- Rädsla Barnen, Sweden;
- IWF, United Kingdom.

We are also very grateful to the following non-EU members of INHOPE, for cooperating in our project:

- ABA, Australia;
- Barnaheill, Iceland;
- NCMEC, United States.

Special thanks go to Mr. Thomas Rickert, President of INHOPE, to Mr. Ian Brown, Administrator, and to the members of the Executive Committee, for their input and suggestions concerning the questionnaire sent to INHOPE members. Please note that the findings and proposals mentioned in this Report do not represent the views of the INHOPE Association.

For the *Area of Intervention C (Awareness and educational initiatives)* UNICEF Innocenti Research Centre is particularly grateful to the following experts and representatives of national governments (in alphabetical order):

- A. Björklund, Ministry of Health and Social Affairs, Sweden;
- M. Brousse, *La Voix de l'Enfant*, France;
- G. Canovas, *Acción contra la pornografía infantil*, Spain;
- J. Carr, *NCH Action for Children*, United Kingdom;
- D. Carstensen, *Save the Children*, Italy;
- D. Cipolla, *Associazione Centro Elis*, Italy;
- A. Davidson, *European Research into Consumer Affairs*, United Kingdom;

- I. De Shrijver, *Childfocus*, Belgium;
- T. Ewbank, *MAPI, Facultés Notre-Dame de la Paix*, Belgium;
- F. Farr, *Associação Portuguesa de Apoio à Vítima*, Portugal;
- I. Geretschlaeger, *NÖ Landesakademie*, Austria;
- J. Hemberg, *Save the Children*, Finland;
- E. König, Bundeskanzleramt/Verfassungsdienst, Austria;
- T. Kyriakides, *Hellenic Consumer Organization, E.K.A.T.O.*, Greece;
- L. Lauridsen, Ministry of Justice, in collaboration with the Ministry of Research and Information Technology and Ministry of Social Affairs, Denmark;
- R. Limper, *Vereniging voor openbaar Oncerwijs*, Netherlands;
- N. Morgan, *Learning and Teaching Scotland*, United Kingdom;
- J. Morrisey, *National Centre for Technology in Education*, Dublin City University, Ireland;
- T. Noten, *ECPAT Netherlands*, Netherlands;
- A. Pappalepore, *Conorzio Hermes*, Italy;
- U. Paschold, Bundesministerium für Familie, Senioren, Frauen und Jugend, Germany;
- K. Pere, Ministry of Transport and Communications, Finland;
- V. Samara, *Extreme Media Solutions Ltd*, Greece;
- D. Ware, Home Office, in collaboration with the Department of Trade and Industry, United Kingdom.

In the preparation of this Report, UNICEF-IRC benefited from the expert contribution of Laurence Fayolle of the European University Institute, Florence.

UNICEF-IRC is also grateful to Sarah Lassner, Marc Suhrcke and Carolina Vizcaino for their support during the course of this research.

3.

EXECUTIVE SUMMARY

This Final Report presents the results of the Study *Child Pornography on the Internet – Evaluating Preventive Measures in order to Improve their Effectiveness in the EU Member States*, funded by the EU Commission under the DAPHNE Programme 2000–2003 (Contract 01/097/c) and carried out by Transcrime, Joint Research Centre on Transnational Crime, Università degli Studi di Trento – Università Cattolica del Sacro Cuore di Milano, in cooperation with Unicef – Innocenti Research Centre, Firenze and Unisys Belgium.

The aim of the Study was to evaluate the effectiveness of the preventive measures in place in EU Member States, in the field of child pornography on the Internet in order to contribute to their improvement. To achieve this aim, the Study set itself the following objectives:

1. to map the preventive measures in place in EU Member States against child pornography on the Internet;
2. to assess (where possible) the level of adherence to EU guidelines of the preventive measures against child pornography in place in EU Member States;
3. to assess the effectiveness of the preventive measures against the child pornography on the Internet in place in EU Member States;
4. to identify good practices in the field of preventive measures against child pornography on the Internet in place in EU Member States and to disseminate them; to identify ways and forms to improve the effectiveness of such measures.⁵

For the purposes of this Study, the term “child pornography” shall mean “pornographic material that visually depicts a child engaged in sexually explicit conduct”.⁶ The concept of child pornography thus defined includes so-called ‘virtual child pornography’,⁷ that is pornographic material created either by manipulating existing pictures or by producing a combined image from different pictures, or even those that are entirely computer-generated.

The term “prevention” was defined as the set of all those measures, whose general goal is to “reduce the level of a crime”. For the purpose of this Study, “preventive measures” were therefore considered “those legislative, regulatory actions and technical devices whose goal (outcome) is to reduce the overall level of pornographic material circulating in Internet”. In the field of child pornography on

⁵ The approved project originally set itself an additional objective, i.e. objective 5) to turn the findings of the evaluation into practical tools to be used by practitioners. After consultation with the partners and having decided during the seminar held in Bruxelles on 15 and 16 January 2004 that the state of art of the topic is still in its infancy, it was decided not to pursue it.

⁶ Communication from the Commission to the Council and the European Parliament, “Combating trafficking of human beings and combating sexual exploitation of children and child pornography” – Proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography, COM (2000) 854 final/2.

⁷ *Manual on Child Pornography Legislation*, research done by Mrs. Conny Rijken assigned by Europol, Trafficking in Human Beings Unit, March 2001, pp. 9–10.

the Internet, prevention is the outcome that can be achieved through different interventions:

- Area of Intervention A: Detection and Control: the main actors in this area are the Law Enforcement Agencies of the EU Member States;
- Area of Intervention B: Self-regulation: the main actors in the field are National Internet Hotlines and Internet Service Providers as they play an important role as institutions directly involved in both the prevention and removal of child pornography on the Internet;
- Area of Intervention C: Awareness and Educational Initiatives: the main actors in the field are governments, NGOs, educators and all the Institutions and bodies working on raising awareness about child pornography on the Internet;
- Area of Intervention D: Technological Measures: technology plays an important role in child pornography on the Internet. On one hand it is an instrument that is exploited by paedophiles to achieve their goals and on the other it is a powerful instrument for the prevention for their illegal activities.

Therefore, the activities undertaken to reach the aim and objectives of the Study were conducted in relation to each of the four above-mentioned Areas of intervention.

The findings of the Study, for each of the above mentioned Areas of Intervention, are as follows:

A) Findings for Area of Intervention A: Detection and Control

The level of adherence of the preventive measures enacted by EU Member States to EU guidelines is quite high. The thematic field of "Criminal Law Justice", "Investigative and Judicial Measures" and "International Cooperation" reach quite a high level of adherence in the majority of EU Member States. The lowest level of adherence is in the thematic field related to the "Liability of Internet Service Providers".

To the contrary, the analysis on the evaluation of preventive measures enacted by EU Member States shows that at the current state of the art of research, it is a very complex task to effectively evaluate the preventive measures related to the Area Detection and Control. The main problem is the paucity of useful data to complete an evaluation. In particular there seems to be a lack of quantitative data, which are essential in order to evaluate the impact of the preventive measures on the reduction of the child pornography material on the Internet.

Where quantitative data are available, they are processed in different ways by the various Specialised Law Enforcement Units in EU Member States. This does not allow a comparative analysis between EU Members States in order to single out which preventive measures are more effective and to check the feasibility of exporting these measures to the other Member States.

As clearly emerges both from the research findings in the evaluation activity and from the expert's opinions in the Working Seminar held in Brussels on 15 and 16 January 2004, the human and material resources made available to the Specialised Law Enforcement Units do not seem to be sufficient to set provide the means to fight child pornography on the Internet.

Some conclusions arise directly from the Working Seminar. In general, experts agreed on the need for a further harmonization of judicial and investigative standards for the collection and usage of digital evidence within EU Member States.

Experts also agreed on the fact that the amount of human and material resources provided to tackle child pornography on the Internet should be increased and, whenever possible, managed in a more efficient manner. In particular they highlighted specific elements already in place that could be improved or modified in order to guarantee the best possible results in tackling child pornography on the Internet. Some of these elements are connected with the organization of the Specialized Units; other issues are related to the exchange of information between Specialized Law Enforcement Units and the other stakeholders (in particular Industry, Hotlines and NGOs) dealing with the fight against child pornography on the Internet.

From an organizational point of view, all the experts agreed on the fact that the Specialized Law Enforcement Units in the different EU Member States play a primary role in investigations into child pornography on the Internet. At international level a network of these Specialized Units already exists. Europol and Interpol are fundamental links in this network allowing the exchange of information from a constantly updated database. This network of Specialised Units could be improved by following the suggestions of the Law Enforcement experts: in particular it is possible to enhance it by increasing the efficiency of communications between the various Units.

In order to improve communications it is possible to intervene at different levels: at the organizational level it is possible to set *ad hoc* points of contact for each Unit, able to receive information, to analyse and to re-direct them to the right office. This would limit the time lost in exchanging data and information.

In order to enhance the network of Specialised Units at an operational level, *ad hoc* training of each Unit on the network is necessary in order to raise the staff's skills and their capability to tackle child pornography on the Internet. During the Seminar, Law Enforcement experts provided many good examples of training in Specialised Units in EU countries. It was, in particular, remarked upon that training should not be a "one shot" period but should take place over a long term period. This would allow the continuous improvement of an agent's knowledge of dealing with new investigations techniques useful to face the challenges of the fast-changing Internet environment.

Another issue, closely related to staff training, concerns to the daily checking of thousands of child pornography images by the staff of the Specialised Units. This negatively impacts the health and safety of the workers and it is necessary to think of remedies to create a safer working environment. Psychological support for the staff could be a possible solution, but it is important to also organize the Unit so that there is a turnover allowing agents to change their function inside the Units. The staff-care issue is also common to other actors in the field, in particular to Hotlines: it is possible to learn from other experiences in order to find the most suitable solutions.

Besides the above listed issues regarding the improvement of the ability of Specialised Law Enforcement Units to fight child pornography on the Internet, there are other important issues regarding the relationship between these Units and the other actors in the same field. One of the most surprising questions raised by the experts during the Seminar is the lack of communication with prosecutors. Paradoxically there is a gap inside the judicial environment due to the fact that

prosecutors do not have the appropriate instruments and means to understand the techniques used by the Specialized Units to gather digital evidence.

The relationship between Law Enforcement and other actors in the field of the prevention child pornography on the Internet (ISPs, Hotlines, NGOs and Institutional bodies dealing with awareness raising) is another topic to that requires addressing. There are many good examples of high standard cooperation between the different actors in the field but important steps have to be made in order to enhance this cooperation. As for the network of Specialized Units, it is important to create single points of contact in order to ease the exchange of information between the different stakeholders. The points of contact should also work as an interface between the different entities at a very practical level. It is possible to consider joint teams of different experts in the field of child pornography during the investigation. As child abuse or child exploitation is a very delicate issue to investigate, psychological support for the person charged with such a crime, for example, could provide for better results for the police.

Finally, it would be important that Law Enforcement agents could offer their experience and knowledge on child pornography on the Internet to raise awareness in the prevention of this specific crime. Additionally their involvement in awareness campaigns could be useful to create trust towards Law Enforcement.

Trust seems to be the key word to enhance the capability of Law Enforcement to fight child pornography on the Internet. Trust from the other actors in the field, trust from citizens that report suspected cases to the local authority, trust from the industry that has to cooperate with Law Enforcement by providing the information required.

What clearly emerged during the discussion in the Seminar was that to improve the efficiency of Law Enforcement preventive measures, as well as those from the other actors in the field of the prevention of child pornography on the Internet, it is important to have continuous feedback from the stakeholders, continuous feedback based on a common language shared by the different entities dealing with the prevention of child pornography on the Internet.

B) Findings for Area of Intervention B: Self-regulation

Effective voluntary codes of conduct carry substantial benefits for governments, the industry and consumers when they are implemented to enforce compliance to control criminal phenomena such as child pornography on the Internet. A huge obstacle to promoting such an approach is its sustainability. Self-regulation is often perceived as a competitive disadvantage as it places compliance burdens on businesses without an immediate return on their investment. However, this way of thinking is accurate only when the codes of conduct are ineffective and fail to provide any real benefits to the industry sector.

As emerged from the research, EU ISPAs are at the beginning of creating a good self-regulatory scheme. One cannot avoid the impression of heterogeneity and sometimes incoherence when reading some rules, which leads one to fear that most could remain empty words. As emerged from the mapping activity, it should be acknowledged that the harmonization of the activities between countries should be the objective of future EU initiatives on self-regulation. However, a prerequisite for such a campaign is the presence within each EU Member State of a reliable Internet Industry referee. The first step required is to support the creation of national regulatory bodies that are able to reach a critical number of market participants by

including the major players, while striking a balance between commercial and law enforcement interests. National ISPAs could play this role, they should, however, strengthen their position in the countries in which they are not the main body by interacting with the majority of Internet Industry stakeholders. In those countries where they are not present, they should be established; conversely, where more than one ISPA exists, the number should be reduced in order to define a single counterpart within the Industry sector that can act as a representative for all the players.

In spite of the fact that ISPA representatives do not like to be addressed as Internet gatekeepers, it is also true that they could play such a role. When tackling child pornography on the Internet, one can state that the ISPs are similar to banks in the fight against money laundering, as they are an independent party that can easily spot suspect transactions. Nonetheless, market constraints clearly affect an ISP's approach, as they are alarmed about being pushed out of the market by unscrupulous providers outside EU borders. The international nature of the Internet clearly raises concerns about this issue, though these should not prevent the industry from engaging in such activities. While these initiatives may be seen as being contrary to their economic interests in the short term, they will provide a return on the investment in the long term. Moreover, several countries are working on codes of conduct and other initiatives that are more stringent than those in Europe, as the Australian Internet Industry (All) code demonstrates.⁸ The All code provides a basis for ongoing cooperation between law enforcement agencies and ISPs in relation to the prevention, detection and investigation of criminal activity perpetrated through the Internet. This code provides a set of procedures for cooperation in order to ensure that all investigative costs and efforts are minimized and equitably divided between the parties involved.

The EU Commission should therefore pursue the harmonization of self-regulatory schemes in all EU Member States as well as provide incoming countries with guidelines and suggestions to develop those schemes. Cooperation between the stakeholders would certainly be enhanced and, at the same time, the quality and number of the initiatives against child pornography would benefit from this improved scenario.

The seminar held in Brussels in January 2004 brought together different expertise from law enforcement, hotline representatives and the Internet industry (mostly ISPA members). The initiative's aim was to discuss the findings of the activities carried out and to develop guidelines to overcome some of the above-mentioned obstacles while defining how an effective self-regulatory scheme should work.

The ISPA membership theme was discussed as a central point in order to develop effective codes of conduct. The fact that several members of national ISPAs are involved in different kinds of businesses entails a higher level of effort when drafting a code that can be applied to all the parties involved. This element, together with the different legal restrictions in force in each EU Member State, discourages the introduction of a code of conduct promoted directly by the EU Commission with the cooperation of various ISPAs. It has been argued that a common code of conduct would not be feasible due to the different levels of development among each of these associations as well as the diverse standards

⁸ IIA, *Cybercrime code of practice* (2003). Retrieved from [http://www.iaa.net.au/cybercrime_code_v2\(cln\).doc](http://www.iaa.net.au/cybercrime_code_v2(cln).doc)

that each of the associations will have created according to their own national legislation.

Although a common EU code of conduct is not considered a viable solution there is still an urgent need to find an alternative path as findings from the mapping activity have disclosed. Participants agreed that a set of common key features should be enacted in order to harmonize the different codes of conduct and enable them to be effective tools to tackle criminal behaviour. For instance, it is vital that a code of conduct includes a review process in order to keep it up-to-date and functional. Although notice and take down procedures operate as reactive measures to child pornography, they should also be considered as key features for a code of conduct and be consistent throughout the EU. Therefore, the involvement of the EU Commission and national government bodies in promoting such harmonization should be encouraged.

Seminar participants rejected the idea of developing a common EU platform for enacting cooperation between ISPs and the law enforcement agencies that carry out investigations. Where not already established, a memorandum of understanding between ISPs and law enforcement agencies would serve to smooth and ease cooperation. Currently, most of the contacts between investigators and ISPs are maintained through informal and personal communications. Each Cyber Crime Unit maintains its own "red line" to contact national ISPs when their help is required. However, this may cause problems to both ISPs, which can be called upon to go further than they are permitted when collecting information, i.e. turn a blind eye to EU rules on personal data protection, as well as law enforcement, which may run the risk of seeing their investigation delayed if their usual contact is not available. It could be useful to develop good protocols for the exchange of information in each country according to its national laws. The agreement signed between the Belgian police forces, the Minister of Justice, the Minister for Telecommunications and the Belgian ISPA could become a template for similar initiatives.⁹

As regards cooperation with law enforcement, a standard form for an information request would be valuable to speed up an ISP's activities when retrieving data. While in some countries, such as the United Kingdom, a standard form already exists, most EU members do not have similar tools. The setting up of a single point of contact between ISPs and law enforcement units in order to avoid processing multiple requests, which all involve the same investigation, would also be advisable.¹⁰ However, the obstacles to developing such initiatives lie in the willingness of ISPs to invest money or find alternative financial support.

Within the context of cooperation between ISPA's and law enforcement, the willingness and capability of ISPs to get involved in the fight against child pornography has been widely discussed. ISPs and other Internet related businesses have often been seen as enterprises composed of technicians who cannot be called upon to work on complicated legal topics related to computer crime and child pornography. There are obviously limits to the interventions that can be requested of ISPA Members. Nonetheless, the EU Commission is currently making efforts to bridge this gap. For instance, the RAND Handbook¹¹ is an easy to use guide that

⁹ Seminar communication (16th January, 2004), Yves Goethal, child pornography coordinator, Federal Police Belgium.

¹⁰ Seminar communication (16th January, 2004), Michael Rotert, EuroISPA President.

¹¹ RAND Europe, (2003) Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, retrieved from <http://www.iaac.org.uk/csirt.htm>.

matches technical descriptions of incidents to the legal framework of the country in question and details procedures for working with law enforcement to respond to incidents. Although it has been developed to help Computer Security Incident Response Teams (CSIRTs) meet their challenges, it could also provide Internet businesses with the legal knowledge they need.

Indeed, ISPA members, namely service providers, access providers and content providers, are not called upon to present definitive solutions in the fight against child pornography but to cooperate to reduce crime opportunities. Following crime prevention theories,¹² ISPA members could be “capable guardians” while helping to reduce the availability of “suitable targets”. As suggested, ISPA members could work on three different preventative approaches:¹³

1. Prevent perpetrators, either abusers or child pornography consumers, accessing the necessary technological infrastructures;
2. Prevent people from accessing child pornography already circulating on the Internet;
3. Prevent children from being contacted by abusers thereby helping the development of a safer environment.

With regards to point one, participants were divided on the effectiveness of acceptable user policies that clearly state the user’s liability for showing/distributing/exchanging illegal materials. Although, it is clear that such a simple measure cannot prevent criminals from pursuing their goals, they could constitute a barrier for simple viewers. As ISPA representatives pointed out, other key players should be scrutinized when looking at the infrastructures used to exchange child pornography, in particular the mobile phone industry. This industry is becoming the new access provider for the Internet. It is now facing the same problems ISPs have been coping with for years. As the Internet is about to go mobile, it may be more difficult to prevent or detect crimes. Hence, the fight against child pornography will soon involve more participants.¹⁴ For instance, search engines should also be closely looked at when dealing with child pornography. Due to their massive archives of Internet web pages and their work as indexers, search engines could help to prevent children from accessing illegal content. In Germany, search engines are requested to work with a Commissioner for youth protection in order to identify which content may not be suitable for underage individuals.

As regards responsibility for accessing illegal content, the main attitude within the Internet industry is to move such responsibility from ISPs to individual users. The results from the questionnaire suggest that content filtering is not useful, demonstrated by the hesitation of ISPs to confirm the utility of filtering software at the ISP level. However, it has been suggested that, as happened with anti-virus

¹² Clarke, R. (1980) Situational Crime Prevention: Theory and Practice, *British Journal of Criminology*, 20, pag. 136–147. and Cohen, L. and M. Felson. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, 44, pag. 588–08.

¹³ Seminar communication (16th January, 2004), Thomas Rickert, INHOPE President .

¹⁴ In January 2004, mobile phone operators in the UK announced a joint code of practice for the self-regulation of new forms of content on mobile phones. Mobile operators have signed up to the code designed to facilitate the responsible use of new mobile phone services whilst safeguarding children from unsuitable content on their mobile phones. A copy of the code is available from the website of each of the operators (Orange, O2, T-Mobile, Virgin Mobile, Vodafone and 3).

software, there could be a market for ISPs providing anti-porn filtering facilities. It should be noted that the market for content filtering systems has not developed at all, as few industries are interested in investing money in such tools, as emerged from the research carried out by Unisys.

Even though ISPA members could provide good gate-keeping services for the Internet, certain content should not be subject to self-regulation schemes for reasons of ethics and democracy. The interpretation of some values cannot be appropriated or usurped by particular interests. As discussed during the seminar, ISPAs cannot be called upon to assess the legitimacy of the content or be the censor of Internet. Conversely, ISPA members should work together to define rules in order to control the access to high-risk services such as chat rooms, peer-to-peer networks and IRC. For instance, strict registration rules for joining IRC services could help in both the identification and traceability of users. Furthermore, national ISPAs could promote the development of common Internet standards. The use of common standards for digital certificates could be an example of how illegal behaviour could be stopped through industry self-regulation. Common standards could be implemented regarding both technological solutions and consumer protection initiatives (i.e. data collection and privacy rights).

C) Findings for Area of Intervention C: Awareness and Educational Initiatives

EU Member States have applied European legislation in a heterogeneous way.

While all governments have some degree of knowledge about the nature and scale of child pornography on the Internet and acknowledge the dangers of the Internet, none consider that the dangers of the Internet may have slowed down the latter's development. Most governmental reports to date deal with general Internet safety issues or more general sexual exploitation of children, and are viewed also as information sources for professionals and/or the general public.

The majority of the countries state that they are involved in the implementation of preventive measures to combat child pornography on the Internet, especially awareness and educational initiatives. However, it seems that few governments have attributed financial support to non-governmental initiatives for awareness raising or education.

Campaigns for safer use of the Internet have taken place in at least eight of the Member States, though some have been partial or limited. It seems that two countries also have plans to launch global national awareness campaigns. National or regional initiatives regarding education of children are in place in ten countries, but their scale varies widely.

The heterogeneity of the measures taken by governments should not necessarily be taken to mean that certain countries are inactive in this field. A review of the five groups of actors selected by UNICEF-IRC – NGOs, Internet providers, education authorities, law enforcement agencies and other bodies – highlights a variety of different approaches to the problem of illegal and harmful use of the Internet. Some actors have followed government initiatives when they exist, others have encouraged a self-regulatory approach by the industry, and others come from the child welfare sector and are particularly proficient in the promotion of awareness projects.

In almost all countries, one or several NGOs are involved in promoting education and/or awareness initiatives. However, some respondents stated that there are so

many activities in this area that it is difficult to estimate numbers, while elsewhere it was difficult to find more than one NGO developing awareness initiatives. The main targets of these initiatives are children and young people. Nine countries confirm the existence of Internet providers involved in promoting education and/or awareness initiatives but, as stated in the Evaluation Report from the Commission in 2001, the efficiency of Hotlines could be increased by making their existence better known to Internet users. Thirteen countries are said to have education authorities involved in awareness and education initiatives. But these campaigns, often launched in the framework of European Projects, are mainly directed at preparing the ground for awareness actions. Implementation of full-scale awareness actions has not always followed. Very few experts are informed about law enforcement agencies being involved in promoting education or/and awareness initiatives. Equally, as concerns other bodies, very few media groups are engaged in awareness or education initiatives as such, but media reports of cases of paedophilia arouse great public concern. Many discussions and round tables have taken place on this issue with wide media coverage.

Eight countries seem to coordinate awareness and education initiatives, but the form of this coordination varies widely from one country to another.

It is noteworthy that the mapping of national preventive measures in place in EU Member States identified at least one European project per country, save apparently Luxembourg. Through its Multi-annual Community Action Plan, the EU is supporting a considerable number of awareness and educational projects and is already in the process of taking stock of lessons learned in protecting and educating children during the implementation of the first phase of the Action Plan (1999-2002).

Although the problem of child pornography on the Internet seems to be very real, its magnitude varies according to the situation in each country. Countermeasures will therefore also be relative. It seems reasonable to assume that the larger the percentage of online users, the greater the chance that there will be a significant proportion of users who are less sophisticated in terms of their computer fluency and general level of education. While the overall level of penetration in the Member States stands at 33%, this figure masks very significant national differences, from Greece with a rate of 13% to Sweden at 51%. The four most populous EU countries – France, Germany, Italy and UK – which comprise 68.3% of total EU population and a similar percentage (just over 71%) of the region's online users, are all in the middle range for penetration (from 28% to 40%), but the proportion of under-17 users, and the time they spend on-line, varies widely from country to country. Campaigns – and their evaluation – need to take these variations into account.

Internet pornography as such is considered variously as desirable, acceptable, a minor nuisance or a major threat. Regional and historical differences and changes are of course substantial. Once the problem has been recognised, the question remains as to what combination of measures could be the most effective to tackle it. While awareness campaigns seem to be one of the most widespread answers to fight child pornography, they can certainly be neither the sole, nor always even the primary, means used. Nonetheless, research shows that across Europe most adults have similar concerns about safety and the Internet, and are looking for similar kinds of information and solutions to provide protection for children against harmful content and use.

In evaluating effectiveness, the main assumption is that the higher and more complete the combination of the four effectiveness indicators – multiplicity of

actors involved, multiplicity of means used, coverage and outreach, and sustainability of projects – the higher the numbers of young users reached. This notwithstanding, and given the global and borderless architecture of the Internet, the most effective preventive measures would be those that can be adapted to the specific nature of the Internet, thereby maximising potential outreach for children and their families.

Multiplicity of actors involved – In nearly all countries, we found more than one actor, but very few have cross-sectoral campaigns involving different actors (government, NGOs, Internet providers, education authorities, law enforcement agencies and European partners). Further, no country seems to have set up effective coordination between these actors. However, with European projects, a first phase of identification of multiplier organisations has been achieved that will contribute to the future implementation of the eSafe programme.

Multiplicity of means used – Five different groups of means were selected: websites, printed leaflets and brochures, TV campaigns, newspapers and radio. Every country has established a website as a result of a governmental or non-governmental initiative. Virtually every country also uses printed leaflets, brochures and/or guides in order to disseminate information about the safer use of the Internet. In contrast, it appears that only seven countries use TV campaigns in awareness and education initiatives. Radio and newspapers are sometimes involved in awareness campaigns but their use could also be greatly improved.

The phase of developing and adapting existing materials and technical solutions is now nearing completion. With a high input from European projects, materials have been selected and successful awareness-raising techniques are or will be translated, adapted and prepared for each country and more generalised use. This constitutes a set of preparatory actions to provide European schoolteachers and future websites with effective means for safe Internet use by children. A word of warning has nonetheless come from the European Parliament which declared in 2002 that ‘the intermediate evaluation of the action plan of 2001, presented by the Commission, revealed that while the European Commission has funded a total of 9 awareness projects, it seems that the specific recommendations on cost-effectiveness were not taken into account.’

In the opinion of many actors in the field, the ‘messages’ should indicate solutions to the problems while at the same time giving information to parents and teachers. Current updated information about the filtering and rating solutions available is vital to complement the awareness messages. Additionally, the messages given to the public should never have an alarmist tone and should not only inform the public about the most negative aspects of the Internet.

Coverage and outreach – Dissemination of information is rarely at national level. Most initiatives seem to be one-off regional or local projects. Through the European projects, after a relatively large-scale pilot testing, plans have been developed to target teachers and other audiences. In this field, we are still at the phase of preliminary dissemination with limited and partial actions. While the foundations for large-scale actions exist in some countries, the campaigns have yet to be launched, and more coordination between projects is needed.

Sustainability of the action – Some countries have established permanent structures, but generally, training programmes in schools concerning safer use of the Internet have not been established on a permanent basis, and the specific question of child pornography is only mentioned in passing, if at all. It is important that ‘awareness’ websites have high visibility and accessibility in major search

engines, and that they are cited or, when necessary, created as part of the campaign. It is also crucial that individual agreements with various portals are reached. All the material and the results of the actions taken for an awareness campaign should be constantly communicated and presented to the multiplier organisations involved, which does not seem to be the case at present.

D) Findings for Area of Intervention D: Technological Measures

The Internet is not a child-friendly environment at all, as children may be exposed at various levels to inappropriate Internet material or experiences through a variety of channels, such as Web pages, e-mail, chat rooms, instant messages, Usenet newsgroups, and peer-to-peer file-sharing connections. Children have to be protected as they are sometimes too confident and too young to understand what is appropriate for them and what is not. Hopefully, many preventive technological devices already exist and are developed nowadays.

However, emphasis must be put on the fact that none of the technologies is 100% effective and that the content of the Internet is, by its very nature, anonymous and volatile. Also, as each individual is different and as the technologies on which the control mechanisms present major differences as well, there is no perfect solution. So choosing the right device depends on various factors and the indicators provided in the present report may help making the right decision.

Nonetheless one has to be aware of the following important facts:

- The Internet is not static, nor is the World Wide Web. New pages are being added to the web at the rate of hundreds of millions every year and just building and maintaining effective filter lists is an immense undertaking. New sites and pages appear every minute and any group or company attempting to prepare comprehensive and complete criteria (filtering, categorisation) lists will always be running behind.
- The criteria lists will never be complete and satisfying because they need to be flexible and adjustable to individual wishes, but cannot, on the other hand be tailored for each individual (as people differ in age, culture, religion, etc.).
- The technologies used are sometimes incapable of distinguishing between information sense and intention (e.g. a sexual solicitation sent by e-mail and a news story about restrictions on online pornography or between a computer virus and a story about a computer virus); this implies that users cannot be sure that content will be rated appropriately and that perfectly innocuous content will not be blocked.
- Systems are easily misled by the use of substitution letters, etc.
- Furthermore, using real-time types of filtering approaches can considerably slowdown system performance. Therefore those filtering techniques based on dynamic examination of content coming from the Internet are suitable for client side use only. From a performance level of expectations point of view, ISP-based control mechanisms have to handle thousands of requests per second, so even simple keyword matching would have trouble operating at this rate. And more complex mechanisms, such as those based on context and image analysis, would simply be impractical.

In order to increase efficiency, technologies have to be used in combination and in layers, and both at the ISP and end-user levels, such as for instance, a combination

of labels and URL lists used at the ISP in conjunction with a final filter at the client level using local lists and/or automated analysis techniques.

In addition to the above, further development of technological devices, extra regulations and the creation of standards are and will remain necessary in order to continuously improve the protection of children against child pornography material.

The technology partners do not necessarily have to evolve just 'for the sake of technology'. It would be profitable for everyone if technology providers adopted an holistic approach regarding the fight against child pornography, as well as regarding other related types of crimes. They could broaden their actions towards other aspects than the purely technological, and towards the other actors in the field of fighting against child pornography

They could pay more attention to the problem of computer literacy, as the ignorance of the user increases his/her risk of being (or having his/her child) victim of child pornography, and more globally, as it may lead to a two-speed society.

For instance, technology providers

- could define (analyse, standardise, automatise) working procedures in order to optimise specific and/or overall collaboration between them (ISPs, hotline managers, device/tool producers) and other partners;
- could promote or improve communication channels with the other partners (eg. working seminars with the police or legislative representatives , discussion forum with research centres, informative websites, ...);
- they could be proactive in terms of information, especially towards end-users and children, by initiating clear and adapted messages popping up on the end-user's screen each time they launch the Internet, for instance;
- they could be included, or at least consulted, in the conception of educational programs for both adults and children (at school), underlining what could be the dangers of the Internet; describing how to use it safely and what are its possibilities, helping everyone to understand each one's responsibilities.

These are only a few suggestions on how technology providers may contribute to the development of a common sense preventive attitude towards the Internet, much like adults very naturally instil in children not to accept sweeties and not to follow unknown persons.

On the basis of the above findings, the following recommendations were drafted. These are divided into sections reflecting the research path: the first are general in the sense that it is possible to address them to the different key stakeholders in the different Areas of intervention. The others specifically deal with each Area of intervention.

General Recommendations

Recommendation n°1

Background and rationale:

The research findings have highlighted the paucity of data enabling a meaningful evaluation of the preventive measures adopted in the field of child pornography on the Internet. Despite the large amount of information processed and made available by the different key stakeholders dealing with child pornography on the Internet, the data currently available are diverse and far from being comparable.

Recommendation:

Action should be taken at an EU level to promote the development of common standards in data gathering procedures in the different Areas of intervention.

Recommendation n°2

Background and rationale:

From the research findings and in particular from the seminar proceedings, it emerged that people working on tackling child pornography on the Internet suffer negative impacts on their health and safety due to the cruel images and delicate situations they have to look at and deal with every day.

Recommendation:

Action should be taken at an EU level to foster initiatives for continuous psychological support for the workers dealing with child pornography on the Internet. Turnover, for example, in this particular working environment could help reducing the negative impact produced by the child abuse images and by the delicate situations workers have to face daily.

**Recommendations for Area of intervention A
(Area Detection and Control)**

Recommendation n°3

Background and rationale:

Differences in national standards for the collection and usage of digital evidence across EU Member States are a very sensitive problem. It often occurs that the legal procedures for the collection of evidence in a certain EU country are regarded as unlawful in other EU Member States. For this reason, courts in a given Member State may reject the evidence collected in another Member State, thus hampering the successful prosecution of the case.

Recommendation:

Action should be taken at an EU level to further harmonize MS legal and procedural standards related to the collection, validity and use of digital evidence in cases of computer crime and computer related crime. This could be achieved through the creation of a *Law Enforcement Certificate* to be accepted in all the EU Member States. This certificate would officially state the parameters within which the evidence was collected, respecting minimum standards to be set on the basis of Civil Rights and Fundamental Freedoms.

Recommendation n°4

Background and rationale:

From the discussion with experts belonging to the Specialised Law Enforcement Units in the European Union it emerged that prosecutors and judges do not always have the appropriate instruments to correctly understand and interpret computer crime related evidence. This may impair the successful prosecution of a given criminal case.

Recommendation:

Action should be taken at an EU level to provide prosecutors and judges with the necessary knowledge to understand the techniques used for the collection of digital evidence and to correctly interpret it. This could be achieved through the setting up of periodic training seminars.

Recommendation for Area of intervention B (Area Self-regulation)

Recommendation n°5

Background and Rationale:

From the research findings it is clear that both public and private bodies are aware of the crucial role that self-regulation – codes of conduct particularly – may play in the prevention of child pornography on the Internet. Nevertheless, existing codes of conduct are still heterogeneous and sometimes incoherent with the purpose of controlling and preventing in specific child pornography on the Internet. This can ultimately affect their effectiveness.

Recommendation:

Action should be taken at an EU level to promote the adoption at MS level of a set of minimum standards for effective codes of conduct. It would be useful, for example, to set clear procedures for cooperation with law enforcement agencies, or effective sanctions to act as a strong deterrent.

Recommendation n°6

Background and rationale:

Notwithstanding the existence of a leading entity such as INHOPE, the European hotline scenario is still highly fragmented. Specifically, the exchange of information between the various hotlines and between hotlines and other key stakeholders in the field of child pornography does not take place on any systematic and routinely organised basis.

Recommendation:

Action should be taken at an EU level to enhance the cooperation, coordination and the exchange of information and data within the hotline network and between hotlines and other key stakeholders.

**Recommendations for Area of intervention C
(Area Awareness and Educational Initiatives)**

Recommendation n°7

Background and rationale:

The research findings highlighted the existence of a large number of actors in the field of awareness and educational initiatives. Unfortunately, it seems that this field suffers from a certain lack of coordination between these actors, which reduces the effectiveness of their efforts to tackle child pornography on the Internet.

Recommendation:

Action should be taken at an EU level to create an EU level organisation acting as an umbrella for the different public and private bodies in the field of awareness and educational campaigns to tackle child pornography on the Internet. In the framework of the initiatives by this organisation it could also be possible to set up a permanent forum for Awareness in which sharing information, exchanging ideas and possibly to set common and EU level strategies to increase the effectiveness of awareness and educational campaigns in EU Member States.

Recommendation n°8

Background and rationale:

As stressed by experts in the field, a need to develop up-to-date awareness campaigns to the fast changing character of the Internet is widely perceived. Specifically, new media such as mobile phones with cameras, are of great concern as they are susceptible to greatly facilitating the production and distribution of pornographic material involving children, and to facilitate communication among paedophiles. Parents and children, as well as the private and public subjects involved in the prevention of child pornography, often lack a complete understanding of these issues.

Recommendation:

The EU Commission should promote the enlargement of the focus of awareness campaigns to include the new media in order to set strategies for effective knowledge-based prevention of the illicit behaviours committed by means of these new technological solutions.

This could be achieved through research projects and educational initiatives aimed to increase knowledge regarding the impact of these instruments on society. It would also be important for the EU Commission to create round tables with all the key stakeholders in the field, such as awareness organisations, NGOs, manufacturers and service providers to act proactively in this field.

**Recommendation for Area of intervention D
(Area Technological Measures)**

Recommendation n°9

Background and rationale:

Even if in this research only the dark side of the Internet emerges, it is important not to demonise this media. The pro-active role that both the Internet new IC technologies can play in tackling child pornography is sometimes underestimated and underused.

Recommendation:

Action should be taken at an EU level to promote the exploitation of the potential offered by the Internet to set strategies in order to increase end-user education regarding child pornography on the Internet and cyber crimes in general. In other words, to consider the Internet as a pro-active instrument for the prevention of on-line child pornography. For this purpose, the EU Commission could encourage the industry and the awareness raising actors to work together in order to improve the technological alphabetisation of Internet end-users.

Recommendation n°10

Background and rationale:

From the research findings and from the discussion with experts in the field, the necessity to create a safer Internet environment clearly emerges. What seems to be most important is the perception of this safer environment for the end-user, starting from the beginning of his/her web surfing and during the whole navigation.

Recommendation:

Action should be taken at an EU level to assess the feasibility of an *EU Safe Site Certificate* to be applied to web sites that are child pornography or child exploitation free, in the sense that they provide completely legal and child oriented material.

The perception of a safe Internet environment is indeed a crucial issue in tackling child pornography on the Internet. An *EU Safe Site Certificate* could be a very pragmatic solution to make the surfer aware that he can trust the virtual place he/she is surfing.

Attention should be paid to set appropriate parameters for this Certificate. It would be advisable to set these parameters after a discussion with the key stakeholders in the field of the prevention child pornography on the Internet and with representatives from Civil Rights Associations in order to avoid any risk of censorship of the Internet content.

4.

AIM AND OBJECTIVES OF THE STUDY

This Final Report presents the results of the Study *Child Pornography on the Internet – Evaluating Preventive Measures in order to Improve their Effectiveness in the EU Member States*, funded by the EU Commission under the DAPHNE Programme 2000–2003 (Contract 01/097/c) and carried out by Transcrime, Joint Research Centre on Transnational Crime, Università degli Studi di Trento – Università Cattolica del Sacro Cuore di Milano, in co-operation with Unisys Belgium and Unicef – Innocenti Research Centre, Firenze.

The aim of the Study was to evaluate the effectiveness of the preventive measures in place in EU Member States, in the field of child pornography on the Internet in order to contribute to their improvement. To achieve this aim, the Study set itself the following objectives:

1. to map the preventive measures in place in EU Member States against child pornography on the Internet;
2. to assess (where possible) the level of adherence to EU guidelines of the preventive measures against child pornography in place in EU Member States;
3. to assess the effectiveness of the preventive measures against the child pornography on the Internet in place in EU Member States;
4. to identify good practices in the field of preventive measures against child pornography on the Internet in place in EU Member States and to disseminate them; to identify ways and forms to improve the effectiveness of such measures.¹⁵

For the purposes of this Study, the term “child pornography” shall mean “pornographic material that visually depicts a child engaged in sexually explicit conduct”.¹⁶ The concept of child pornography thus defined shall include the so-called ‘virtual child pornography’,¹⁷ that is pornographic material created either by manipulating existing pictures or by producing a combined image from different pictures, or even entirely computer-generated.

The term “prevention” was defined as the set of all those measures, whose general goal is to “reduce the level of a crime”. For the purpose of this Study, “preventive measures” were therefore considered “those legislation, regulation, actions and technical devices whose goal (outcome) is to reduce the overall level of pornographic material circulating in Internet”. In the field of child pornography on

¹⁵ The approved project originally set itself an additional objective, i.e. objective 5) to turn the findings of the evaluation into practical tools to be used by practitioners. After consultation with the partners and having decided during the seminar held in Bruxelles on 15 and 16 January 2004 that the state of art of the topic is still in its infancy, it was decided not to pursue it.

¹⁶ Communication from the Commission to the Council and the European Parliament, “Combating trafficking of human beings and combating sexual exploitation of children and child pornography” – Proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography, COM (2000) 854 final/2.

¹⁷ *Manual on Child Pornography Legislation*, research done by Mrs. Conny Rijken assigned by Europol, Trafficking in Human Beings Unit, March 2001, pp. 9–10.

the Internet, prevention is the outcome that can be achieved through different interventions:

- Area of Intervention A: Detection and Control: the main actors in this area are Law Enforcement Agencies of the EU Member States;
- Area of Intervention B: Self-regulation: the main actors in the field are National Internet Hotlines and Internet Service Providers as they play an important role as institutions directly involved in both the prevention and the removal of child pornography on the Internet;
- Area of Intervention C: Awareness and Educational Initiatives: the main actors in the field are governments, NGOs, educators and all the Institution and bodies working on the rising awareness about child pornography on the Internet;
- Area of Intervention D: Technological Measures: technology plays an important role in child pornography on the Internet. On one hand it is an instrument that is exploited by paedophiles to achieve their goals and on the other it is a powerful instrument for the prevention for their illegal activities.

Therefore, the activities undertaken to reach the aim and objectives of the Study were conducted in relation to each of the four above-mentioned Areas of intervention.

5.

OPERATIONAL DEFINITIONS

The research findings in the different Areas of Intervention are based on common key concepts regarding the prevention on child pornography on the Internet. These common key concepts follow the European Commission's indications (Hippocrates Programme) and are listed below:

- '*child pornography*' shall include 'pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct'.¹⁸ The concept of child pornography defined in this way also includes so-called 'virtual child pornography'¹⁹, that is pictures that have been altered, such as morphed images of natural persons, or even those that are entirely computer-generated.
- '*minor*' is defined as 'all persons under 18 years of age'. A lower age-limit is allowed, which shall be no less than 16 years.²⁰
- '*self-regulation*' is defined as the regulation created by private bodies who are called to enforce the regulation by themselves. It includes 'all systems which can efficiently help the flow of illegal content on the Internet, including Internet hotline reporting mechanism and codes of conducts'.²¹
- '*awareness raising*' is defined as 'any activity intended to bring a particular issue to the attention of a group or groups (*target*), normally with the aim of encouraging attitudinal or behavioural change'. '*Awareness campaign*' is defined as 'a mobilisation for a specific duration, normally using mass communication techniques, with the aim of promoting raised awareness of a particular issue'.
- '*education initiative*' is defined as 'a measure intended to empower or enable a group or groups vis-à-vis a particular issue through the provision of information and/or training'. Within this context, '*sub-national*' refers to the level of government administration immediately below the central level, normally equated with regional government;
- '*national plan of action*' refers, in the context of this research, to 'any plan developed by a country in order to implement the Stockholm Agenda for Action adopted at the First World Congress against the Commercial Sexual Exploitation of Children in 1996'. The plan is normally drawn up by governmental and child care agencies;
- '*prevention*' is to be considered as the set of all those measures, whose general goal is to 'reduce the level of a crime'. For the purpose of this Project, 'preventive measures' should therefore be considered 'those legislative, regulative actions and technological measures the goal of which is to reduce the

¹⁸ Council of Europe, *Convention on Cybercrime*, ETS n. 185, art. 9.2.

¹⁹ *Manual on Child Pornography Legislation*, research carried out by Mrs. Conny Rijken assigned by Europol, Trafficking in Human Beings Unit, March 2001, pp. 9-10.

²⁰ Council of Europe, *Convention on Cybercrime*, ETS n. 185, art. 9.3.

²¹ Decision n. 276/1999/EC of the European Parliament and of the Council adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, published in the Official Journal L 33, 6 February 1999, Action line 1.

overall level of pornographic material circulating on the Internet'. The Project therefore focuses on on-line child pornography, and does not attempt to include the on-line stalking of children, which relates to quite different mechanisms, actors and consequences and which is also subject to different laws.

6.

INTRODUCTION

Child pornography on the Internet is a priority in the EU agenda due to the negative impact this criminal phenomenon has on society in general, and in particular on the weaker elements of society itself: children.

In fact, exploited children can suffer physical, psychological and social consequences such as long-lasting physical and psychological trauma, disease (including HIV/AIDS), violence/abuse, drug addiction, unwanted pregnancy, malnutrition, social ostracism, poverty and in many cases, death.

Unfortunately new technologies such as Internet and Information and Communication Technologies (ICT) in general, can offer new opportunities for criminals in order to exploit children and to exchange child pornography material in very cheap and efficient ways.

These technologies play an important role also in facilitating contact offending against children and an easy access to a large population of viewers, collectors and possessors of child pornography material, with the consequence to increase the demand for new child abuse images to be produced.

Prevention seems to be the key concept to tackle child pornography on the Internet: prevention can in fact interrupt this vicious circle, reducing the general demand and amount of child pornography material circulating on the Internet. For these reason it is important to evaluate the preventive measures in place in EU Member States in order to improve their effectiveness in tackling child pornography on the Internet.

How to assess this effectiveness?

Due to the uncertainty of data on demand and supply of child pornography and more on internet the assessment of the effectiveness of measure for combating it cannot rely on traditional measures for assessing the impact of policies. Reasoning in terms of *inputs* defined as any additional human, physical and financial resources used to undertake a Project, *outputs*, defined strictly as the direct products of the implementation process, and *outcomes* defined as the consequences of the intervention, an effective policy is that can achieve the most relevant part of outcomes in proportion to the inputs allocated and the outputs produced. Being impossible for the lack of data an evaluation of the situation of child pornography on internet before and after the intervention this research makes an assumption on the methodology for assessing the effectiveness of the policies considered. That is that considering that assuming that more specified outputs (known) are realised more outcomes (unknown) are produced the research will look to the policies that produce outputs. They can be summarised as follow:

- *deterrence* (i.e., increasing the risks for criminals of being detected, incriminated and punished, and having the illicit proceeds of their crimes confiscated);
- *protection of potential victims* (i.e., making children and their families aware of and protect them from the risks of exposure to child pornography on Internet);
- *reduction of opportunities for criminals* (i.e. eliminating the opportunities that facilitate the commission of child pornography crimes on the Internet).

The general outcome of the research should be the reduction of the overall level of child pornography material on the Internet.

Even if each of the four Areas of intervention contributes to the accomplishment of this outcome, at the current state of the art, it is not possible to determine how much each area contributes to its achievement. In other words, this outcome cannot be measured, because of a lack of consistent information.

As a consequence, this Study identifies and lists those measures that are most capable of being effective in producing outputs. The achievement of outputs are measured through the use of objective indicators of effectiveness and, where these are not available, subjective indicators.

What can be assumed is that the higher the effectiveness of the measures within a single Area of Intervention, the better the outputs produced and the outcome achieved.

7.

FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION A (DETECTION AND CONTROL) BY TRANSCRIME

7.1 INTRODUCTION

This Section aims to evaluate the effectiveness of the preventive measures enacted by EU Member States in the area of Detection and Control (Area of Intervention A).

This section deals with the research findings related to the first three *Objectives* of the Study, i.e.:

1. mapping the preventive measures in place in EU Member States against child pornography on the Internet;
2. assessing the level of adherence to EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States;
3. assessing the effectiveness of the preventive measures against child pornography on the Internet in place in EU Member States.

7.2 METHODOLOGICAL STEPS

Objective 1 (*mapping the preventive measures in place in EU Member States against child pornography on the Internet*) has been reached through the following steps:

- *collection and review of the EU guidelines against child pornography on the Internet as regards Detection and Control*: the EU guidelines form the basis of the entire analysis within this Area of intervention. These guidelines provide for operational definitions as well as guidance to EU Member States on how to tackle child pornography on the Internet. In the Area Detection and Control, the EU guidelines aim to directly impact on the legislative framework of EU Member States, and, for this reason, they can be considered as practical suggestions for the creation of national legislative frameworks based on common definitions with the necessary elements in order to cope with child pornography on the Internet. Where specific guidelines were not directly provided by EU documents, they were extrapolated, by researchers, through discussion with experts and through the analysis of available literature;
- *mapping of the preventive measures in place in EU Member States related to Area of intervention Detection and Control, by means of a questionnaire based on the EU guidelines and aimed at understanding which of them have been enacted by EU Member States*: the questionnaire for the mapping of the preventive measures in place in EU Member States against child pornography on the Internet was drafted following the categorisation of the EU guidelines in the Area of Detection and control.²²

²² The questionnaire on the mapping activity is available in Chapter 13, Annex 1.

The questionnaire was drafted following the categorisation of the EU guidelines in the Area of Detection and control. In particular it was mainly composed of 4 parts:

1. *Criminal Law Measures*: this first part aims to understand whether specific child pornography offences have been enacted and, if so, which conducts are criminalised and which sanctions are provided;
2. *Investigative and Judicial Measures*: this second part aims to acquire information on the existence and on the structure of specialised law enforcement units and on the use of special means of investigation;
3. *International co-operation*: this third part aims to gather information about the investigation and the prosecution of child pornography offences on the Internet at international level;
4. *Responsibility of Internet Service Providers*: this final part aims to collect information related to the role of ISPs in the dissemination of child pornography material over the Internet.

The draft of a first questionnaire was discussed with law enforcement officials and a member of the Steering Committee, Mr. Bjerne Clarberg of Europol, in order to test its validity, and was subsequently sent to the experts in the law enforcement units dealing with child pornography cases in all EU Member States, who were identified with the cooperation of Europol.

The information acquired with the questionnaire, supplemented by an analysis of secondary sources, is summarized in a series of synoptic tables, which are available in Chapter 13, Annex 2.

Objective 2 (*assessing the level of adherence to EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States*) has been reached through the following step:

- *evaluation of the level of adherence to the EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States, based on information gathered through the answers to the questionnaire on the mapping activity of the preventive measures in place in EU Member States*. This information has been used to calculate an Index of Adherence of EU Member States to the EU guidelines against child pornography on the Internet.

The index of adherence shows if and how the EU guidelines have been applied in the different Member States.

In order to calculate this index, the adherence of each EU Member State to each EU guideline was investigated. The answer 'Yes' was assigned in case of adherence of a Member State to a given EU guideline, while the answer 'No' was assigned in case of non-adherence.

The index has a scale of 0 to 100. The higher this Index, the higher the adherence of EU Member States to EU guidelines against child pornography on the Internet.

The second step involved assigning the value '1' to each answer 'Yes' and the value '0' to each answer 'No' in relation to the existence or non existence of a given guideline in the Member State's legislation.²³ In case a given guideline is

²³ The same weight was applied to all guidelines.

composed of more than one constitutive element, the values 1 or 0 were assigned to each of the possible options. The average of the elements was then calculated in order to assign a final value to the guideline.²⁴

Objective 3 (*assessing the effectiveness of the preventive measures against child pornography on the Internet in place in EU Member States*) has been reached through the following steps:

- *drafting of a second questionnaire, based on the findings of the mapping activity, to evaluate the effectiveness of the preventive measures developed by EU Member States:* this questionnaire was disseminated through the same network (where possible) of experts that replied to the first questionnaire. As for the mapping activity, both the dissemination of the questionnaire and the gathering of the answers were successful due to the collaboration of Mr. Bjerne Clarberg from Europol.

As this questionnaire aimed to evaluate the effectiveness of the preventive measures against child pornography on the Internet in place in EU Member States, it is important to define what evaluation of effectiveness means in this context. It is important to underline that this evaluation of effectiveness does not rely on direct indicators. The evaluation of the effectiveness of these preventive measures is mainly based on the perception of experts who work daily in the field of child pornography on the Internet with instruments and resources, provided by the legal framework they belong to.

Due to their knowledge and expertise, these experts can provide an evaluation of what is effective and what it is not.

In this context effective means the capability of a measure to produce different outputs, in particular:

- *deterrence:* i.e., increase the risk of criminals being detected, incriminated and punished, and having the illicit proceeds of their crimes confiscated);
- *protection of potential victims:* i.e., making children and their families aware of, and protecting them from exposure to, child pornography on Internet);
- *reduction of opportunities for criminals:* eliminating those opportunities that facilitate the commission of child pornography on the Internet.

As for the mapping activity, the questionnaire was divided into four different sections, representing different thematic fields:

- *Criminal Law Measures;*

²⁴ See, for example, the following guideline, contained in the Council of Europe Convention on Cybercrime: 'Existence of measures establishing as criminal offences the following conducts related to child pornography:

- a) producing child pornography for the purpose of its distribution through a computer system;
- b) offering or making available child pornography through a computer system;
- c) distributing or transmitting child pornography through a computer system;
- d) procuring child pornography through a computer system for oneself or for another;
- e) possessing child pornography in a computer system or on a computer-data storage medium'.

In this case the values 1 or 0 were assigned to each of the five elements a) to e), which were therefore treated in the same way as autonomous guidelines.

- *Investigative and Judicial Measures;*
- *Cooperation at EU level;*
- *Quantitative Data.*

The thematic fields are different from those of the questionnaire for the mapping activity.

In particular the field of *Cooperation at EU level* includes questions regarding International Cooperation and the questions regarding the Liability of the Internet Service Providers.

The *Quantitative Data* field, which was not in the questionnaire for the mapping activity, aims to collect the largest possible amount of quantitative data about the preventive measures against child pornography on the Internet in place in EU Member States, in the area of detection and control.

The first three sectors of the questionnaire are structured on a Likert scale in order to allow respondents to give a numeric value to their answers. The Likert scale goes from a minimum value of 1 to a maximum value of 4; where 1 means not at all effective, 2 means quite effective, 3 means effective and 4 means very effective.

The *Quantitative Data* sector was designed to allow the respondents to insert all the quantitative data available regarding a non-definitive list of specific topics.

- *analysis of the answers to the questionnaire in order to evaluate the effectiveness of the preventive measures mapped:* to develop this step three different types of analysis were carried out, i.e.:
 - a) the first type of analysis was a macro one, the aim of which was to depict the different distribution of non-valid answers in the different sections (statistically called 'dimensions') of the questionnaire;
 - b) the second type of analysis aimed to single out an index of effectiveness of the measures evaluated through the various questions of the questionnaire. Each question was analysed in order to identify which has the higher average in the Likert scale and, consequently, seems to be more effective according to the experts.
 - c) the third type of analysis focused on the types of quantitative data sent by experts in the field.

The next step involved the discussion and finalisation of the research findings from the above activities with experts in the field of child pornography prevention on the Internet during the Working Seminar held in Brussels in January 2004.

Finally, a series of Recommendation based on the research findings directly addressed to the EU Commission and to the key stakeholders in the field of child pornography prevention on the Internet, were developed.

The findings from the above steps are in the following sections.

7.3 EU GUIDELINES AGAINST CHILD PORNOGRAPHY ON THE INTERNET AS REGARDS AREA OF INTERVENTION DETECTION AND CONTROL

For the purpose of the Study, EU guidelines are, in general, documents produced directly by European Union Institutions and by the Council of Europe Convention on Cybercrime, sustained by the Council of the European Union in the Common Position of 27 May 1999.

The EU guidelines selected concerning Detection and Control measures are the following²⁵.

Criminal Law Measures (Thematic Field)

1. Existence of a definition of 'child pornography' which includes pornographic material that visually depicts: a) a minor/child engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct (CoE Convention, art. 9.2);
2. Existence of measures establishing as criminal offences the following conducts related to child pornography:
 - a) producing child pornography for the purpose of its distribution through a computer system;
 - b) offering or making available child pornography through a computer system;
 - c) distributing or transmitting child pornography through a computer system;
 - d) procuring child pornography through a computer system for oneself or for another;
 - e) possessing child pornography in a computer system or on a computer-data storage medium (CoE Convention, art. 9.1);
3. Existence of a definition of 'minor', including all persons under 18 years of age. If a lower age-limit is required, this can be not less than 16 years of age (CoE Convention, art. 9.3);
4. Existence of measures requiring confiscation, where appropriate, of the instruments and proceeds of child pornography offences (Joint Action 1997, Title II.A.d);
5. Existence of measures establishing corporate liability, either administrative or criminal (Joint Action 1997, Title II.A.c, CoE Convention, art. 12);
6. Existence of measures providing for the temporary or permanent closure of establishments which have been used or intended for committing child pornography offences (Joint Action 1997, Title II.d).

Despite the existence in EU documents of guidelines concerning sanctions for child pornography offences, these were not taken into account because they are of a very general nature. Both the Council of Europe Convention on Cybercrime and the 1997 Joint Action mention *effective, proportionate and dissuasive criminal penalties which include deprivation of liberty*. A wide variety of sanctions are applied by EU Member States regarding this issue. Moreover, the Council of the European Union

²⁵ The identification of EU guidelines in this Area of Intervention was last updated in 2002, as this part of the project is included in the Intermediate Report of the Project delivered in April 2003.

has not yet been able to reach an agreement on sanctions for child pornography offences.

Investigative and Judicial Measures (Thematic field)

7. Existence of a specialised unit within law enforcement authorities to deal with information on suspected production, processing, distribution and possession of child pornography (Council Decision 2000, art. 1.2);
8. Existence of measures encouraging Internet users to inform law enforcement authorities on suspected distribution of child pornography material on the Internet (Council Decision 2000, art. 1.1);
9. Existence of forms of cooperation between the specialised law enforcement unit and private foundations or associations which combat child pornography (Joint Action 1997, Title II I);
10. Existence of a multi-disciplinary approach which implies co-ordination among the authorities responsible for the fight against the sexual exploitation of children (Ministerial Departments, police forces, judicial authorities specialised in the matter, public bodies with responsibility in the matter (Joint Action 1997, Title II.H);
11. Existence of measures ensuring that the national services (e.g. immigration, social security, tax authorities), which are likely to have relevant experience in the context of sexual exploitation of the children, co-operate with the authorities responsible of the investigation and punishment of child pornography (Joint Action 1997, Title II.G);
12. Existence of the measures necessary to ensure that adequate investigation powers and techniques are available to enable child sexual exploitation and child pornography to be investigated and prosecuted effectively (Joint Action 1997, Title II.E);
13. Existence of measures empowering the competent authorities to search or access a computer system or part of it and computer data stored within, and computer-data storage medium in which computer data may be stored (CoE Convention, art. 19.1);
14. Existence of measures empowering the competent authorities to seize or similarly secure computer data accessed (CoE Convention, art. 19.3)
15. Existence of measures allowing law enforcement authorities to defer action if and as long as tactically necessary, for instance with a view to getting at those behind the criminal operations, or at networks (child pornography rings) (Council Decision 2000, art. 1.3);
16. Existence of measures enabling the competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system (CoE Convention, art. 16.1);
17. Existence of measures enabling the competent authorities to oblige the person in possession of stored computer data to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days (CoE Convention, art. 16.2);

18. Existence of measures ensuring the expeditious preservation of traffic data and its expeditious disclosure to the competent authorities (CoE Convention, art. 17.1);
19. Existence of measures empowering the competent authorities to order a person to submit specified computer data in that person's possession or control, and to order a service provider offering its services on its territory to submit subscriber information (CoE Convention, art. 18.1);
20. Existence of measures empowering the competent authorities to collect traffic data in real-time or to compel a service provider to collect or co-operate in the collection of traffic data (CoE Convention, art. 20.1);
21. Existence of measures empowering the competent authorities to collect content data in real-time or to compel a service provider to collect or co-operate in the collection of content data (CoE Convention, art. 20.1).

International cooperation (Thematic field)

22. Existence of provisions allowing direct transmission or requests for assistance between locally competent authorities (Joint Action 1997, Title III.D);
23. Existence of measures allowing, in urgent circumstances, to make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail (CoE Convention, art. 25.3);
24. Existence of measures allowing the spontaneous supply to other Member States of information useful to begin or carry out an investigation (Joint Action 1997, Title III.H and CoE Convention, art 26.1);
25. Existence of measures establishing jurisdiction over child pornography offences where:
 - a) the offence is committed in whole or in part within its territory; or
 - b) the offender is one of its nationals; or the offence is committed for the benefit of a legal person established in the territory of that Member State (CoE Convention, art. 22).

Liability of Internet Service Providers (Thematic field)

26. Existence of measures which impose a duty on Internet providers to advise the competent authorities of the specialised law enforcement unit of child pornography material of which they have been informed or of which they are aware and which is distributed through them (Council Decision 2000, art. 3 a);
27. Existence of measures which impose a duty on Internet providers to withdraw from circulation child pornography material of which they have been informed or of which they are aware and which is distributed through them, unless otherwise specified by the competent authorities (Council Decision 2000, art. 3 b);
28. Existence of measures which impose a duty on Internet providers to retain traffic-data, where applicable and technically feasible for such time as may be specified under the applicable national law, to allow the data to be made available for inspection by the criminal prosecution authorities (Council Decision 2000, art. 3 c);

29. Existence of measures which impose a duty on Internet providers to set up their own control systems for combating the production, processing, possession and distribution of child pornography material (Council Decision 2000, art. 3 d).

7.4 EVALUATING THE LEVEL OF ADHERENCE OF EU MEMBER STATES LEGISLATION TO THE EU GUIDELINES

This section presents the findings from the evaluation of the level of adherence to the EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States. In order to do so, an Index of Adherence of EU Member States to the EU guidelines against child pornography on the Internet was calculated.

The index of adherence shows if and how the EU guidelines have been applied in the different Member States. The higher this Index, the higher the adherence of EU Member States to EU guidelines against child pornography on the Internet.

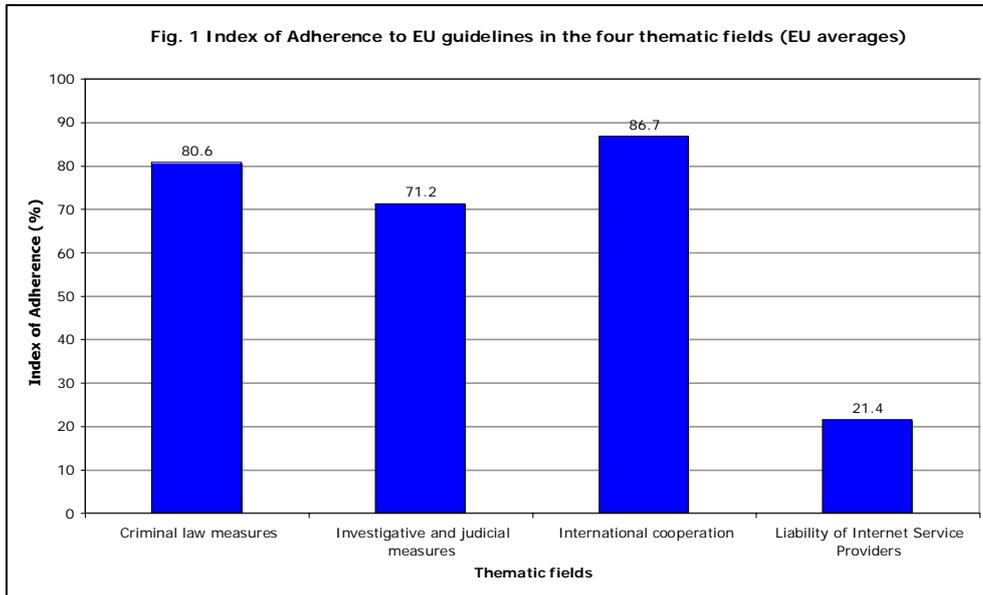
Table 1 shows the Index of Adherence of EU Member States to EU Guidelines in the four thematic fields identified.

Table 1

Index of Adherence to EU guidelines in the four thematic fields (EU averages)

EU Member States	Thematic fields			
	Criminal law measures	Investigative and judicial measures	International Cooperation	Liability of Internet Service Providers
Austria	83.3	-	100.0	0.0
Belgium	100.0	88.0	100.0	75.0
Denmark	75.0	76.0	100.0	50.0
Finland	84.6	52.0	75.0	0.0
France	100.0	76.0	75.0	0.0
Germany	66.7	76.0	100.0	25.0
Greece	92.3	75.0	75.0	-
Ireland	92.3	44.0	100.0	0.0
Italy	92.3	92.0	75.0	0.0
Luxembourg	92.3	16.0	100.0	0.0
Netherlands	69.2	89.5	100.0	0.0
Portugal	38.5	88.0	100.0	0.0
Spain	61.5	56.0	25.0	50.0
Sweden	84.6	68.0	100.0	75.0
United Kingdom	76.9	100.0	75.0	25.0
<i>European Union average</i>	80.6	71.2	86.7	21.4

The indexes of adherence of EU Member State legislations to EU Guidelines in the four thematic fields are graphically represented in Figure 1.



Adherence to EU guidelines in the four thematic fields

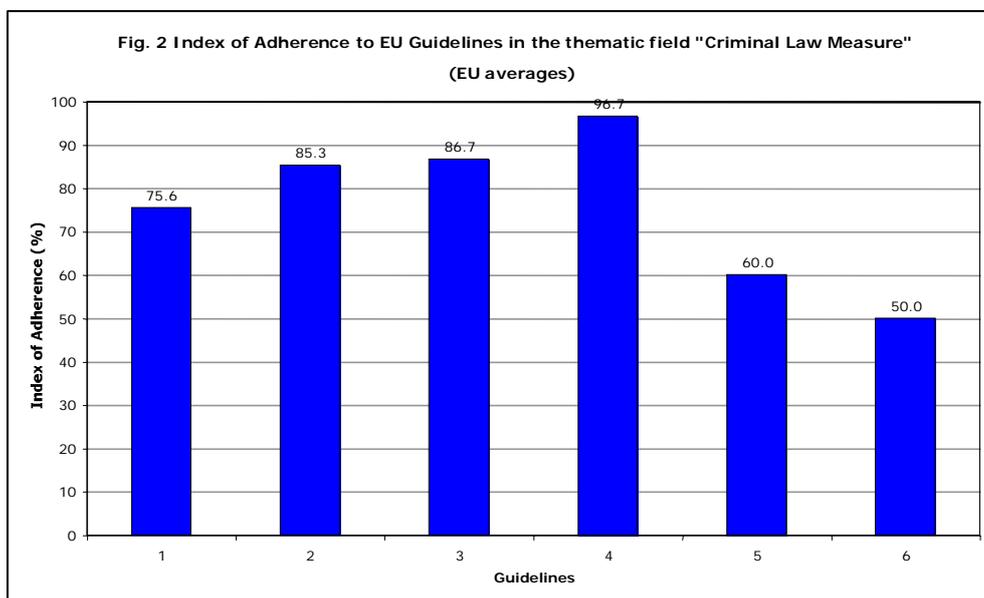
EU Member States show a high level of adherence to EU guidelines in at least two of the four thematic fields identified;

The highest level of adherence to EU guidelines is found in thematic field 'International cooperation' (Index of Adherence 86.7);

There also a high level of adherence in the thematic field 'Criminal Law Measures', even if it is lower than the former (Index of Adherence 80.6);

The thematic field 'Liability of internet Service Providers' shows the lowest level of adherence to EU guidelines (Index of Adherence 21.4).

Figure 2 shows the level of adherence of EU Member States to the specific EU guidelines in thematic field of ‘Criminal Law Measures’.



Level of adherence to EU guidelines in thematic field ‘Criminal Law Measures’ (EU averages)

Highest level of adherence:

Guideline n. 4 (Existence of measures requiring confiscation, where appropriate, of the instruments and proceeds of child pornography offences) – Index of Adherence 96.7;

Guideline n. 3 (Existence of a definition of ‘minor’, including all persons under 18 years of age. If a lower age–limit is required, this can be not less than 16 years of age) – Index of Adherence 86.7;

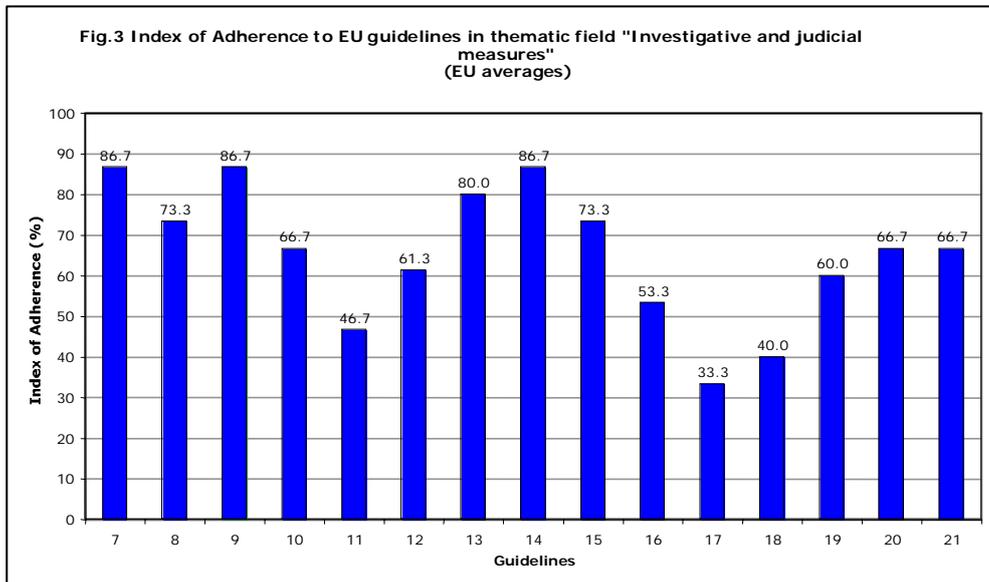
Guideline n. 2 (Existence of measures establishing as criminal offences the following conducts related to child pornography: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another; e) possessing child pornography in a computer system or on a computer–data storage medium) – Index of Adherence 85.3

Lowest level of adherence:

Guideline n. 5 (Existence of measures establishing corporate liability, either administrative or criminal) – Index of Adherence 60.0.

Guideline n. 6 (Existence of measures providing for the temporary or permanent closure of establishments which have been used or intended for committing child pornography offences) – Index of Adherence 50.0.

Figure 3 shows the index of adherence of EU Member States to EU Guidelines in the thematic field of 'Investigative and Judicial Measures'.



Level of adherence to EU guidelines in the thematic field 'Investigative and Judicial Measures' (EU averages)

Highest level of adherence:

Guideline n. 7 (Existence of a specialised unit within law enforcement authorities to deal with information on suspected production, processing, distribution and possession of child pornography), guideline n. 9 (Existence of forms of cooperation between the specialised law enforcement unit and private foundations or associations which combat child pornography) and guideline n. 14 (Existence of measures empowering the competent authorities to seize or similarly secure computer data accessed) – Index of Adherence 86.7;

Guideline n. 13 (Existence of measures empowering the competent authorities to search or access a computer system or part of it and computer data stored within, and computer-data storage medium in which computer data may be stored) – Index of Adherence 80.0.

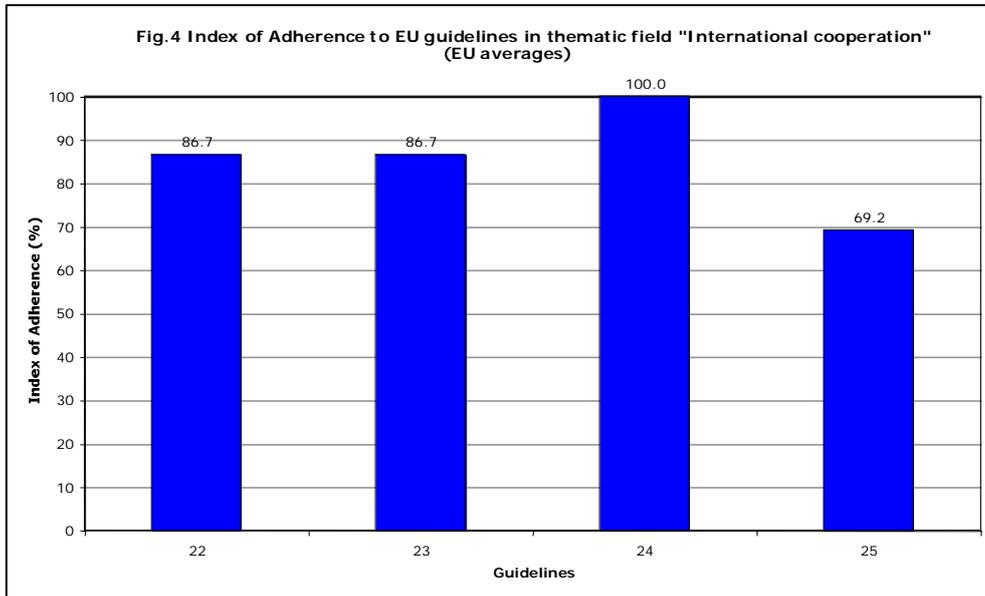
Lowest level of adherence:

Guideline n. 11 (Existence of measures ensuring that the national services (e.g. immigration, social security, tax authorities), which are likely to have relevant experience in the context of sexual exploitation of the children, co-operate with the authorities responsible of the investigation and punishment of child pornography) – Index of Adherence 46.7.

Guideline n. 18 (Existence of measures ensuring the expeditious preservation of traffic data and its expeditious disclosure to the competent authorities) – Index of Adherence 40.0.

Guideline n. 17 (Existence of measures enabling the competent authorities to oblige the person in possession of stored computer data to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days) – Index of Adherence 33.3.

Figure 4 shows the index of adherence of EU Member States to EU guidelines in the thematic field of 'International Cooperation'.



Level of adherence of EU Member States to EU guidelines (EU averages)

Highest level of adherence:

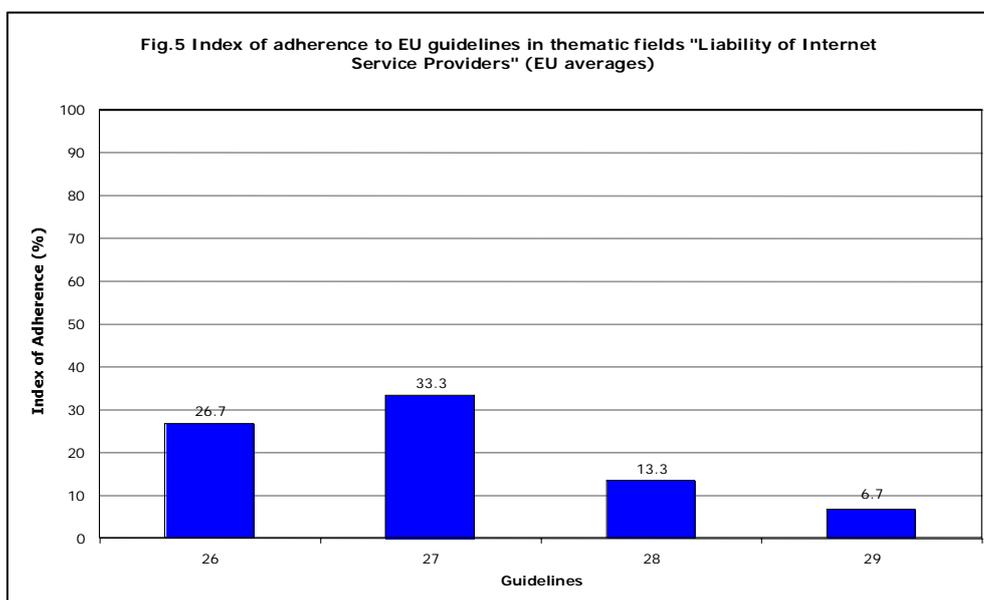
Guideline n. 24 (Existence of measures allowing the spontaneous supply to other Member States of information useful to begin or carry out an investigation) – Index of Adherence 100.0;

Guideline n. 22 (Existence of provisions allowing direct transmission or requests for assistance between locally competent authorities) and guideline n. 23 (Existence of measures allowing, in urgent circumstances, to make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail) – Index of Adherence 86.7;

Lowest level of adherence:

Guideline n. 25 (Existence of measures establishing jurisdiction over child pornography offences where: a) the offence is committed in whole or in part within its territory; or b) the offender is one of its nationals; or c) the offence is committed for the benefit of a legal person established in the territory of that Member State) – Index of Adherence 69.2.

Figure 5 shows the index of adherence of EU Member States to EU guidelines in the thematic field of 'Liability of the Internet Service Providers'.



Level of adherence of EU Member States to EU guidelines in the thematic field 'Liability of Internet Service Providers' (EU averages)

Highest level of adherence:

Guideline n. 27 (Existence of measures which impose a duty on Internet providers to withdraw from circulation child pornography material of which they have been informed or of which they are aware and which is distributed through them, unless otherwise specified by the competent authorities) – Index of Adherence 33.3;

Guideline n. 26 (Existence of measures which impose a duty on Internet providers to advise the competent authorities of the specialised law enforcement unit of child pornography material of which they have been informed or of which they are aware and which is distributed through them) – Index of Adherence 26.7;

Lowest level of adherence:

Guideline n. 29 (Existence of measures which impose a duty on Internet providers to set up their own control systems for combating the production, processing, possession and distribution of child pornography material) – Index of Adherence 6.7.

To sum up the findings from the analysis of the level of adherence of EU Member States to EU guidelines against child pornography on the Internet, the thematic field 'International cooperation' is the one where the highest level of adherence to EU guidelines is to be found (index of adherence 86.7). This may be due to the fact that cooperation channels among EU Member States have already been established and developed over the last few years to investigate organised crime, money laundering and other similar offences, and have now been effectively extended to crimes involving child pornography.

EU Member States also show a high level of adherence to EU guidelines regarding *Criminal Law Measures* (index of adherence 80.6). It therefore seems that EU Member States have harmonised their legislation to a high degree, and are already in compliance with the related articles of the Council of Europe Convention on Cybercrime (which, as already mentioned, has still not entered into force).

The thematic field where a lower level of adherence is to be found, even though it is not much lower than the two previous ones, is that of '*Investigative and Judicial Measures*' (index of adherence 71.2). This may be due to the fact that many of the guidelines selected have been extrapolated by the Council of Europe Convention on Cybercrime. It seems to be the case that many of the countries that have signed the Convention (all EU Member States with the exception of Denmark and Luxembourg) are still in the process of adapting their legislation to the requirements of the Convention.

Finally, it is evident from the above analysis that very few EU Member States have enacted specific legal provisions regarding the criminal or civil liability of Internet Service Providers. The index of adherence of EU Member States to EU guidelines in thematic field 'Liability of Internet Service Providers' is in fact 21.4. It is important, however, to establish whether similar provisions have been introduced in codes of conduct, i.e. self-regulatory instruments adopted by national associations of Internet Service Providers. The existence of provisions in these codes would compensate for the absence of corresponding legal provisions. A specific part of the analysis concentrated on investigating the level of adherence of EU Member States to guidelines regarding codes of conduct, follows in Section 2 of this Report dealing with the Area of intervention B (Self-regulation).

7.5 EVALUATING THE EFFECTIVENESS OF THE PREVENTIVE MEASURES IN PLACE IN EU MEMBER STATES AGAINST CHILD PORNOGRAPHY ON THE INTERNET

This evaluation was carried out on four different thematic fields:

- *Criminal Law Measures;*
- *Investigative and Judicial Measures;*
- *Cooperation at EU level;*
- *Quantitative Data.*

The data gathered through the questionnaire on these four thematic areas have been processed with three different kind of analysis.

The high level of non-valid answers in the section of *Cooperation at EU level* needs an in-depth analysis.

It must be emphasised that this sector includes questions on co-operation at European level (questions 29–30) and questions regarding cooperation between Law Enforcement agencies and the ISPs (questions 30–31–32–33). In many cases this second type of cooperation has to be at a EU level because a Law Enforcement agency needs to co-operate with an ISP located in a different European country.

Looking at the distribution, the level of non-valid answers is particularly consistent in this second set of questions.

Referring to all the questionnaires, it is not possible to understand the reasons for the different distribution of the non-valid answers through the different dimensions by an analysis of the answers, simply because most of the questionnaires do not provide a reason for the non-answered questions.

A hypothesis very close to reality could be the fact that, in some cases, it is not possible to answer the question because the measure analysed does not exist in the country. In this case the question should be posed in a different way, asking how the expert would consider the introduction of a certain measure in order to tackle child pornography on the Internet.

The results from this initial analysis of the distribution of non-valid answers, could suggest that the analysis of the fields of *Criminal Law Measures* and *Cooperation at EU level*, needs further study and that other questions should be asked in order to understand the reasons that do not allow the experts to give valid answers and provide a possible solution for this.

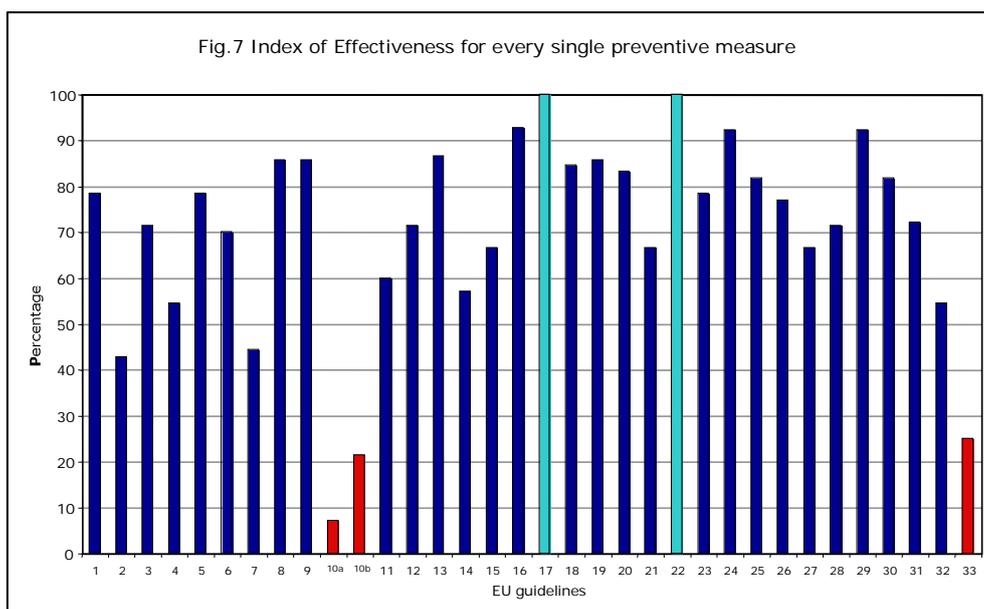
Index of effectiveness for each preventive measure

The second type of analysis aims to identify the index of effectiveness of the measures evaluated through the various questions in the questionnaire.

This index shows the level of effectiveness of a single measure. It is expressed as a percentage and its value is calculated by considering the number of positive values (numeric values of 3 and 4 on the Likert scale) given to a specific measure divided by the number of respondents to the question.

For example, the index of effectiveness of question 24 is high because 9 out of 11 respondents gave it a positive value (3 or 4 on the Likert scale) therefore its percentage value is 81,8%.

The figure below (Fig.7) shows the index of effectiveness for each measure evaluated in the questionnaire.



The percentage value clearly shows that the measures taken into consideration generally have a high level of effectiveness and the all the respondents agree on the effectiveness of measures 17²⁷ and 22²⁸.

There are few measures with a very low level of effectiveness; in particular there is a low level of effectiveness in answers related to questions 10a, 10b and 33. Question 10a and 10b are related to the adequacy of human and economic resources devoted by each country to tackle child pornography on the Internet. Question 33 is related to the existence of a measure that imposes a duty on Internet Service Providers to set up their own control systems to combat the production, processing, possession and distribution of child pornography material. In this case the level of effectiveness is certainly low but the low number of respondents to this specific question (8 out of 15) must also be emphasised.

This element will be deeply discussed in the next type of analysis, which focuses on the mean level of effectiveness of the measures evaluated through the questionnaire.

The analysis of the mean value of effectiveness per question

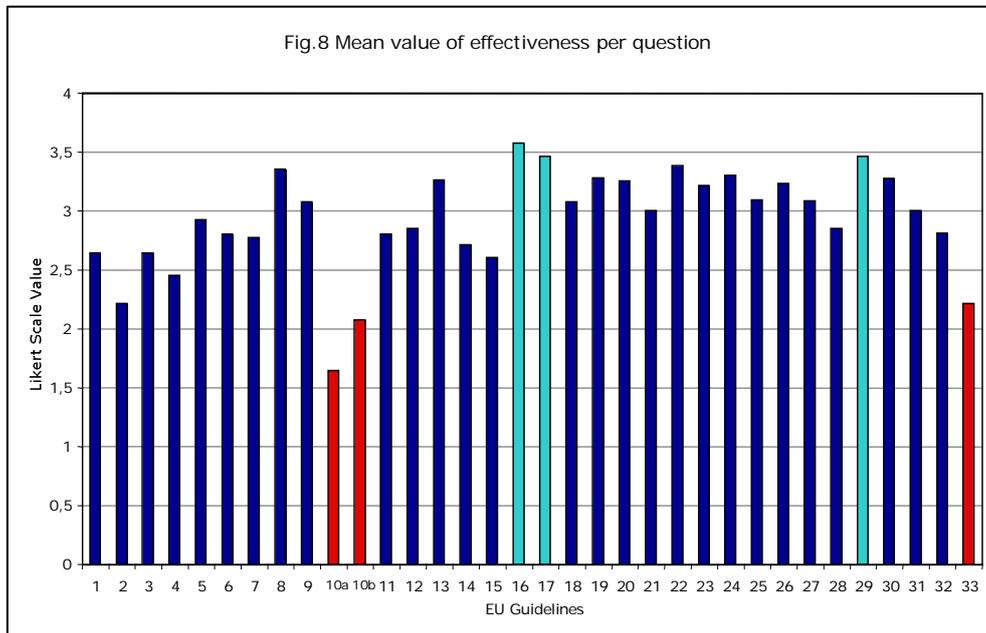
Considering that each question aims to evaluate the effectiveness of a specific mapped measure, it is important to calculate the mean of every answer in order to define the numeric value of its effectiveness at a European level.

²⁷ Question 17: According to you, if any legislative provision, or other measures, exists in your country empowering competent authorities to seize, or similarly secure computer data they have accessed, how do you evaluate its usefulness in tackling child pornography on the Internet?

²⁸ Question 22: According to you, if any measure exists in your country empowering competent authorities to order a service provider offering its services on its territory to submit subscriber information relating to such services, how do you evaluate its usefulness in tackling child pornography on the Internet?

This numeric value is calculated on the sum of each value given by the experts to a specific question, divided by the number of the states that gave a valid answer.

The mean of every question is summarised in the graph below (Fig.8):



The calculation of the mean is based on the number of respondents and it is essential to consider that, in some cases, there were a very low number of valid answers to a specific question. For example, only 9 experts out of 15 answered question 7 and only 8 experts out of 15 answered question 33.

However, the different number of valid answers does not impact on the mean because the mean, in this context, shows the level of effectiveness of a measure that exists and is applied in a specific country.

It means that, only if the measure exists it is possible to evaluate whether it is effective or not.

As for the index of effectiveness, the lowest mean value was given to question 10a and 10b, the questions aimed to evaluate the adequacy of the human and material resources devoted by a country to tackle child pornography on the Internet.

The highest level of mean, given to question 16, 17 and 29, confirms the parallelism between the results of the mean analysis and the analysis of the index of effectiveness.

The same approach of mean per question can also be applied at the sectors level. In this situation, as shown in the table below (Fig. 9), the highest level of effectiveness is in the sector of *Cooperation at EU level*. This means that all the measures mapped in this specific field, where measurable, have a significant level of effectiveness.

On the other hand the lowest level of effectiveness, based on the perception of the experts interviewed, is in the *Criminal Law Measures* sector.

The *Investigative and Judicial Measures* sector, has a medium level of effectiveness, but seems to be the most representative for the high level of valid answers, with the highest average number.

Fig.9 Mean per sector²⁹

Dimensions	Mean per Sector / Average Numerousness
Criminal Law Measures	2.63 / 12.28
Investigative and Judicial Measures	3.01 /13.57
Cooperation at European Level	2.93 / 11.3

Expanding the analysis to the overall results, it is necessary to calculate the mean of all the answers, in order to understand the general perception of the whole set of preventive measures enacted to tackle child pornography on the Internet.

The following table shows the overall mean of the whole set of questions (Fig. 10):

Fig. 10 Overall Mean on three sectors

Dimensions	Overall Mean / Overall numerousness
Criminal Law Measure, Investigative and Judicial Measures, Cooperation at European level	2.92 / 12.91

Once again, if the maximum level of effectiveness is 4, the overall mean shows that all the preventive measures enacted to tackle child pornography, considered in a very large prospective, have a low level of effectiveness.

Quantitative Data

The *Quantitative Data* part is the last section at the end of the questionnaire, aimed to gather quantitative data on some specific topics listed: for example the number of people investigated/arrested/judged or convicted for child pornography offences, the number of people sanctioned with a prohibition to exercise activities related to the supervision of children and other topics.

The analysis of this section shows a consistent shortage of information.

Unfortunately only few questionnaires were filled in with quantitative data related to the topics in this section and these are too few to be useful. In some cases experts provided an explanation for this lack stating that they do not have these kinds of statistics or that they would have to extract these data from the general crime statistics.

This lack of statistical data should be taken into serious consideration. This kind of data would provide concrete support for the opinions of the experts. Thus, if an expert suggests that one particular measure is effective the data could be used to justify such an opinion. Therefore this type of data should be collected in future evaluation studies.

The analysis of the questionnaires on the evaluation of the preventive measures enacted by the EU Member states, in the Detection and Control Area, in order to tackle child pornography on the Internet, provides a large amount of information. An analysis of the questionnaire is certainly useful to convert the expert's perception about the effectiveness of a measure enacted to fight child pornography

²⁹ In the figure Numerousness implies the number of valid-answers received to the Questionnaire.

on the Internet, into a numeric value. The numeric values are simple indicators of what works and what does not, and, for this reason, it is not easy to get behind the numeric value to understand its meaning.

The more effective measures seem to be those regarding the investigational power of law enforcement agencies. In a few cases clear indications emerge from the analysis, for example all the experts agree on the paucity of human and material resources provided by Member States to tackle child pornography on the Internet.

The lack of quantitative data should create great concern and it is necessary to understand the main causes for such a deficit.

If it is possible to affirm that the questionnaire provides interesting information regarding the evaluation of effectiveness of the preventive measures in place in EU Member States against child pornography on the Internet, it is now important to go further by asking the experts to clarify the reasons that led them to choose one number rather than the other, especially in the cases in which the value chosen represents a low level of effectiveness.

7.6 CONCLUSIONS

At the end of this Section regarding the Area of intervention Detection and Control it is possible to synthesize some conclusions both from the research findings of the research and from the information gathered from the experts during the Working Seminar.

Starting from the research findings of the mapping activity, it is possible to affirm that the level of adherence of the preventive measures enacted by EU Member States to EU guidelines seems to be quite elevated.

The thematic field of “Criminal Law Justice”, “Investigative and Judicial Measures” and “International Cooperation” reach a quite high level of adherence in the majority of EU Member States. The lowest level of adherence is in the thematic field related to the “Liability of Internet Service Providers”, but for an-dept analysis of this particular field it is possible to refer to Area of intervention Self-regulation, Section 2 of this Report.

On the opposite, the analysis on the evaluation of preventive measures enacted by EU Member States highlight that actual State of the Art of the research it is very complex to effectively evaluate this kind of preventive measures related to the Area Detection and Control. The main problem seems to be the paucity of data useful to complete an evaluation. In particular there seem to be a lack of quantitative data, which are essential in order to evaluate the impact of the preventive measures on the reduction of the child pornography material on the Internet.

Where quantitative data are available, they seem to be processed in different ways by the different Specialised Law Enforcement Units in EU Member States. This does not allow a comparative analysis between EU Members States in order to single out which preventive measures are more effective and to check the feasibility of exporting these measures to the other Member States. Transferring effective preventive measures to the incoming countries would be important in order create a European standard for data gathering.

As clearly emerges both from the research findings in the evaluation activity and from the expert's opinions in the Working Seminar held in Brussels on the 15 and 16 January 2004, human and material resources addressed to the Specialised Law Enforcement Units seem not to be sufficient to set appropriate means in order to fight child pornography on the Internet.

Some conclusions arise directly from the Working Seminar and are related to important aspects of tackling child pornography on the Internet in the Area Detection and Control.

The Working Seminar grouped at the same table different actors working in the field of child pornography prevention on the Internet: the different areas of intervention were represented by many high level experts who contributed with their knowledge and experience to the success of the discussion.

This variety of experts from different areas surely contributed to a multi-prospective analysis of the child pornography on the Internet.

Regarding the Area of Intervention Detection and Control, it must be underlined that, in general, experts agree on the fact that child pornography should remain a priority in the Law Enforcement investigation.

For this reason they would ask for an effort from the European Institutions towards the harmonization of the judicial and investigative power within the EU Member States.

This harmonization is particularly important in evidence gathering procedures, which are different among the EU Member States. It often happens that evidences legally collected in a EU country, are considered unlawful, and consequently rejected, from another EU Member State.

This mainly happens for evidences gathered by under-cover or *provocateurs* agents, evidences considered lawful only in those EU countries which foreseen this kind of specific investigative agents.

Law Enforcement experts also agree on the fact that the amount of human and material resources to tackle child pornography on the Internet should be increased but they also suggest that it is possible to manage in a better way the resources already available.

In particular they highlighted specific elements already in place, that have to be improved or modified in order to guarantee the best results possible in tackling child pornography on the Internet.

Some of these elements are connected with the organization of the Specialized Units; other issues are related to the exchanging of information between Specialized Law Enforcement Units and the other stakeholders (in particular Industry, Hotline and NGOs) dealing with the fighting of child pornography on the Internet.

From the organizational point of view, all the experts agree on the fact that the Specialized Law Enforcement Units in the different EU Member States play a primary role in the child pornography on the Internet investigations.

At international level a network of these Specialized Units already exists. Europol and Interpol are fundamental knots of this network allowing the exchange of information from constantly updated database.

This network of Specialised Units can be surely improved following the suggestions of the Law Enforcement experts: in particular it is possible to enhance it increasing the efficiency of communication between the different Units.

In order to increase the communication it is possible to intervene at different level: at the organizational level it is possible to set *ad hoc* points of contact for every single Unit, able to receive information, to analyse and to re-direct them to the right office.

This should limit the time loss in exchanging data and information.

In order to enhance the network of Specialised Units at operational level, an *ad hoc* training of every single Unit within the network is necessary in order to raise the staff's skills and the capability to tackle child pornography on the Internet.

During the Seminar, Law Enforcement experts provided with many good examples of training in Specialised Units in EU countries. Due to the different structure and organization of the police forces in the it is not possible to set a common framework for training but it is possible to provide for general indications.

In particular training does not have to be a one spot training but should be structured on long term period: for example every five or six months it would be useful for agents of the Unit to follow course on specific topic related to their work.

This should allow continuous improvement of agents' knowledge in dealing with the new investigations techniques useful to face the challenges of the fast-changing Internet environment.

From the discussion with the experts, another issue, strictly related to the staff training emerged: staffs of these Specialised Units have to work checking daily thousands of child pornography images. This kind of activity negatively impact on the health and safety of the workers and it is necessary to think to remedies in order to create a safer working environment.

A psychological support for the staff can surely be a possible solution, but it is important also to organize the Unit with a turnover allowing the agents to change their function inside the Units.

The staff-care issue is also common to other actors in the field, in particular to Hotlines: it is possible to learn from other experiences in order to find the most suitable solutions.

Besides the above-listed issues regarding the improvement of the ability of the Law Enforcement Specialised Units in fighting child pornography on the Internet, there are other important issues regarding the relationship between these Units and the other actors in the same field.

One of the most surprising questions raised from the experts during the Seminar is the lack of communication with the prosecutors: paradoxically there is a gap inside the judicial environment due to the fact that the prosecutors do not have the appropriate instruments and means to understand the evidences or the techniques used by the Specialized Units to gather the evidences.

During the Seminar, experts reported clear examples regarding this issue and they also argued that if the specialization of the prosecutors raises serious questions when dealing in general with Cybercrime, it has to be considered a main issue in tackling child pornography on the Internet.

The relationship between Law Enforcement and other actors in the field of child pornography on the Internet prevention (ISPs, Hotlines, NGOs and Institutional bodies dealing with awareness rising) was a key element in the discussion.

There are many good example of high standard co-operation between the different actors in the field but important steps have to be done in order to enhance this co-operation.

As for the network of Specialized Units, it is important to create single points of contact in order to ease the exchange of information between the different stakeholders.

The points of contact should work as an interface between the different realities also at a very practical level. It is possible to think about joint teams of different experts in the field of child pornography during the investigation: as child abuse or child exploitation is a very delicate issue to investigate, a psychological support to the person charged with such a crime, for example, can provide for better results for the police.

Finally Law Enforcement agents would offer their experience and their knowledge on the child pornography on the Internet, to raise awareness in the prevention of this specific crime. Their involvement in awareness campaigns in schools for example, could be useful to create trust towards Law Enforcement.

Trust seem to be the key word to enhance the capability of the Law Enforcement to fight child pornography on the Internet: trust from the other actors in the field, trust from citizens that have to report the suspect cases to the local authority, trust from the industry that have to cooperate with Law Enforcement providing the required information.

What clearly emerge during the discussion in the Seminar was that to improve the efficiency of the Law Enforcement preventive measure, as well as those from the other actors in the field of prevention of child pornography on the Internet, it is important to have continuous feedback from the stakeholders, continuous feedback based on a common language shared by the different realities dealing with the prevention of child pornography on the Internet

8.

FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION B (SELF-REGULATION) BY TRANSCRIME

8.1 INTRODUCTION

This Section aims to evaluate the effectiveness of self-regulation initiatives against child pornography on the Internet enacted by EU Member States (Area of intervention B). The initiatives analysed belong to two separate areas, namely a) Internet Service Providers (ISPs) and b) National Internet hotlines.

The reason why these two areas are the main focus of this area of intervention is because of the fact that the EU Commission itself has identified both national Internet Service Providers Associations (ISPAs) and National Internet hotlines as important actors within the 'soft' solutions to combat child pornography on the Internet.

It is worth being mentioned that, as this is a dynamic area, and the institutions that participate in self-regulation (i.e. ISPAs and National Internet hotlines) are still in the process of defining best practices, the mapping activities and, by default, the evaluations are not comprehensive. In fact, many activities may have been instituted after the results of the research activities were processed, consequently these results must be viewed in the same light and must be updated and changed to reflect the activity of the Internet industry.

This Section includes the research findings related to the first two *Objectives* of the Project, and develops in specific the third one:

1. mapping the preventive measures in place in EU Member States against child pornography on the Internet;
2. evaluating the level of adherence to EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States;
3. evaluating the effectiveness of the preventive measures against child pornography on the Internet in place in EU Member States.

8.2 METHODOLOGICAL STEPS

Objective 1 (*mapping the preventive measures in place in EU Member States against child pornography on the Internet*) has been reached through the following steps:

- *collection and review of EU guidelines pertaining to ISPAs and National Internet hotlines in relation to child pornography on the Internet.*
- *based on these guidelines, mapping of the activities in the area of child pornography on the Internet prevention for both ISPAs and National Internet hotlines. As far as the initiatives developed by Internet Service Provider Associations (ISPAs) are concerned, the analysis was confined only to the codes of conduct adopted. In fact, codes of conduct can be considered as the text of reference where all the most important rules of self-regulation are enclosed and systematised. As regards the methodology, relevant information was collected*

by surfing the Internet and analysing existing secondary sources. This method allowed researchers not only to collect the information needed, but also to determine the amount and quality of the information available to end users who may be interested in contacting such associations. As far as the initiatives developed by National Internet hotlines are concerned, a questionnaire was administered to Internet hotlines established in EU Member States.

Objective 2 (*evaluating the level of adherence to EU guidelines of the preventive measures against child pornography on the Internet in place in EU Member States*) has been reached through the following step:

- *evaluation of the level of adherence to the EU guidelines by EU Member States.* This was done by calculating an Index of Adherence of EU Member States to the EU guidelines against child pornography on the Internet.

The index of adherence shows if and how the EU guidelines have been applied in the different Member States.

In order to calculate this index, the adherence of each EU Member State to each EU guideline was investigated. The answer 'Yes' was assigned in case of adherence of a Member State to a given EU guideline, while the answer 'No' was assigned in case of non-adherence.

The index has a scale of 0 to 100. The higher this Index, the higher the adherence of EU Member States to EU guidelines against child pornography on the Internet.

The second step involved assigning the value '1' to each answer 'Yes' and the value '0' to each answer 'No' in relation to the existence or non existence of a given guideline.³⁰ In case a given guideline is composed of more than one constitutive element, the values 1 or 0 were assigned to each of the possible options. The average of the elements was then calculated in order to assign a final value to the guideline.

Objective 3 (*assessing the effectiveness of the preventive measures against child pornography on the Internet in place in EU Member States*) has been reached through the following step:

- *evaluation of effectiveness of the initiatives mapped for both ISPAs and National Internet hotlines through the analysis of the answers to evaluation questionnaires, as well as of secondary source material.*

The concept of evaluation is common to the analysis of both ISPAs and National Internet hotlines, and is of particular relevance for the Project. According to English et al,³¹ evaluation studies are carried out for a variety of reasons such as determining the impact of an existing program, to provide feedback and facilitate program management, to obtain guidance or to modify inputs and processes, to clarify the program philosophy as well as to assist in program development. All of these dimensions are measured using different tools. It is important, however to keep in mind that most evaluation methodologies have been created for use in a small community and with very specific criteria. There are a variety of evaluations that can be conducted depending on the needs of

³⁰ The same weight was applied to all guidelines.

³¹ English B., Cummings R., Straton R. (2002), "Choosing an evaluation model for community crime prevention programs", in *Crime Prevention Studies*, 14, pp. 119-169.

the body requesting the evaluation as well as the resources and time available in which to conduct the evaluation.

According to the purposes of this Study, the types of evaluations to be carried out in this study should be evaluations of effectiveness of the identified prevention strategy. These evaluations are therefore primarily monitoring evaluations, which focus on programme outcomes in order to provide feedback to key stakeholder groups. Considering this evaluation will eventually be used to create best practices and tool-kits to the many participants an objective goal-based approach combined with subjective expert opinions (when possible) will be utilized. In light of the fact that the majority of evaluations are conducted in small areas with very clear criteria, the ability to conduct an international evaluation of strategies requires more flexibility and certainly has substantial limitations.

This stated, the evaluation of effectiveness for the area of self-regulation uses a mix between desk and self-evaluation methodology. When it is possible, experts in the various ISPAs and Internet hotlines were contacted and asked a series of questions that were both subjective and objective in nature. In addition, secondary sources were consulted in order to provide a more complete overview of the services provided. This evaluation methodology clearly has some limitations in that the recipients of the programmes or services were not contacted in order to evaluate the programme's effectiveness from their point of view.

The next step involved the discussion and finalisation of the research findings from the above activities with experts in the field of child pornography prevention on the Internet during the Working Seminar held in Brussels in January 2004.

Finally, a series of Recommendation based on the research findings directly addressed to the EU Commission and to the key stakeholders in the field of child pornography prevention on the Internet, were developed.

The findings from the above steps are in the following sections.

8.3 INTERNET SELF-REGULATION IN THE EUROPEAN UNION: AN OVERVIEW

In early autumn 2003, Microsoft announced that it was clamping down on unregulated chat rooms to prevent those places from becoming safe havens for sex predators. Most commentators recognized this announcement as a sign of private companies' powerlessness to cope with the sexual exploitation of adults and children on the Internet. More recently, the rise in concern about sex related crimes also led the Singapore Information and Communications Minister, Lee Boon Yang, to ask national Internet providers to follow Microsoft's example and shut down all the services they were not able to closely control.³²

If self-regulation 'occurs when those [who are] regulated design and enforce the rules themselves', the above episode might be seen as an extreme form of such regulation applied by the private sector. However, the strategy to close all those services that cannot be controlled clearly appears to be a last resort to stop sexual exploiters. Indeed, self-regulation could be a preventive mechanism against illegal

³² Agencie France Press, *Singapore calls for global Internet chat room crackdown*, 10 November 2003. Available at <http://www.yahoo.com/news>.

and harmful behaviours, which can ultimately damage both operators and users. The objective of self-regulation is to control and regulate a certain sector (Internet, TV media, advertising industry, etc) through non-binding guidance and stakeholder participation. Industry clearly prefers this form of government as it operates without binding the operators to overly restrictive rules, while taking into account the commercial and social differences of the parties concerned. While national law regulation and command-and-control solutions are often perceived to be effective but rigid, self-regulation is seen as an accommodating response in order to reflect industrial tendencies in real time as well as being flexible enough to cover behaviours not previously addressed. Sanctions can be tougher in a self-regulatory system than in hard law solutions and, in some cases, compliance is greater as companies voluntarily join the scheme.

Self-regulation is not a new phenomenon and many codes of conduct and best practices have been developed over the years. However, as Haufler³³ points out 'the trend toward self-regulation went relatively unnoticed until recently. This may be in part because the phenomenon itself is difficult to see.' The digital era has produced a new wave of self-regulatory initiatives, which have been contributing to sustaining Internet development. There are various reasons for this renaissance including the costs of a strict hard law regulation, the industry's desire for flexible norms and a common belief that the Internet should not be subjected to any type of governmental control.

Even though the discussion about the effectiveness of self-regulation is ongoing, it is clear that different forms of regulation need to coexist in order to address the various aspects of the digital world. Self-regulation should be part of the strategies to regulate on-line activities, including illegal behaviours such as the sexual exploitation of children. Aware of the need for such a multi-layer approach, national and international regulatory bodies have included self-regulation in their frameworks to stop the flow of child pornography on the Internet.

The EU Commission has focused its attention on self-regulation since the beginning of its campaign against child pornography on the Internet. In 1999, Council Decision 276/EC adopting the Safer Internet Action Plan points out that industry self-regulation and the increase of industry awareness 'will play a crucial role in consolidating that safer environment and contribute to removing obstacles to the development and competitiveness of the industry concerned'.³⁴ Self-regulatory organisations bring together the expertise of their members in sectors which are often 'too new' to be effectively regulated through command-and-control solutions. Those organisations are an invaluable source of information, knowledge and experience and they constitute a forum for expressing the interests of the various actors and contribute to forming public opinion. For these reasons, the EU Commission stressed the importance of their participation in the making of legislation in order to facilitate wide acceptance of new standards. These guidelines

³³ Haufler V. (2001), *A public role for the private sector: industry self-regulation in a global economy*, Carnegie Endowment for International Peace, Washington D.C., p. 9.

³⁴ Decision n. 276/1999/EC of the European Parliament and of the Council adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, published in the Official Journal L 33, 6 February 1999, pp. 1-11.

have been reinforced in the recent follow up of the Safer Internet Action Plan (2003–2004).³⁵

Under the Safer Internet Action Plan, the EU Commission sponsored the Selfregulation.info project (IAPCODE) run by the Oxford University Programme for Comparative Media Law and Policy.³⁶ This project aims to collect and analyse self-regulatory and co-regulatory schemes as well as codes of conduct and best practices pertaining to the Internet and, for comparison, other relevant areas such as e-commerce, film and video, broadcasting, press and advertising codes. The IAPCODE project is also meant to provide technical assistance to self-regulatory bodies and industry groups seeking to design and/or implement codes of conduct. This advisory task should also be accomplished by developing public understanding on self-regulation and by taking part in discussions on self-regulation at national and international levels.

The role of self-regulation is highlighted in many documents produced by EU bodies about child pornography on the Internet. Article 3 of the EU Council Decision (2000, 29 May) on child exploitation on the Internet, states, 'Member States shall engage in constructive dialogue with industry and examine appropriate measures, of a voluntary or legally binding nature, to eliminate child pornography on the Internet'.³⁷ These initiatives emphasize how self-regulation involves a number of stakeholders within the industry sectors: Internet Service Providers (ISPs), mobile operators, telecom regulators and software developers. The EU Council widely recommends the establishment of a national framework for self-regulation by the operators of online services and the cooperation of industries and other parties concerned (i.e. Internet users and customer associations) in the drawing up of codes of conduct for the protection of minors and human dignity applying to the provision of online services. To meet this target the new Safer Internet Action Plan (2003–2004) foresees the development of a Safer Internet Forum in order to stimulate the 'networking of the appropriate structures within EU Member States and developing links with self-regulatory bodies outside Europe'.

The Council of Europe is working on a path similar to the one followed by the EU Commission. In Recommendation 8 (2001) on self-regulation concerning cyber content, the Committee of Ministers points out that 'Member states should encourage the establishment of organisations which are representative of Internet actors, for example Internet service providers, content providers and users' and 'should encourage such organisations to establish regulatory mechanisms within their remit, in particular with regard to the establishment of codes of conduct and the monitoring of compliance with these codes'.³⁸ In 2001, the Directorate General on Human Rights within the Council of Europe sponsored research into self-regulation and user protection against illegal or harmful content on new communications and information services. Both the Council of Europe and the EU Commission focused their attention on self regulatory bodies which could be

³⁵ Safer Internet Action Plan Work Programme 2003–2004. Available at http://www.europa.eu.int/information_society/programmes/iap/index_en.htm.

³⁶ Extensive information on the IAPCODE project is available at <http://www.selfregulation.info>.

³⁷ Council Decision of 29 May 2000 to combat child pornography on the Internet, published on the Official Journal L 138, 9 June 2000, p. 1.

³⁸ Recommendation (2001) 8 of the Committee of Ministers to member States on self-regulation concerning cyber content: self-regulation and user protection against illegal or harmful content on new communications and information services. Available at <http://cm.coe.int/ta/rec/2001/2001r8.htm>.

defined as representative of the Internet industry and the mechanisms they have enacted to protect users from illegal and harmful content.³⁹

Although, significant parts of the initiatives focus on the creation of codes of conduct, the European Commission was farsighted enough to know that the different stakeholders needed a way to receive information from the public and to relay it in a fast and efficient way amongst each other. The Safer Internet Action Plan and the subsequent communications⁴⁰ state that there must also be a way to monitor the content of the Internet. One of those methods includes a network of hotlines throughout Europe. Hotlines provide an important service as information gatherers and disseminators. In sum, they should be a central point of contact for the public and be able to work effectively with ISPAs as well as law enforcement in order to reduce the amount of child pornography on the Internet. Although not strictly related to content monitoring, hotlines, because of their privileged role with the public, provide a perfect venue for awareness raising activities related to the risks and benefits associated with the Internet.

A review of the initiatives taken by European Commission and the Council of Europe, shows that particular attention is focused on a variety of self-regulatory schemes as a means of reducing the amount of child-pornography available on the Internet. This multi-layered approach is reflected in the analyses of the codes of conduct developed by ISPAs as well as National Internet hotlines.

³⁹ The research findings are available at http://www.coe.int/T/e/human_rights/.

⁴⁰ Decision n. 276/1999/EC of the European Parliament and of the Council adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, published in the Official Journal L 33, 6 February 1999, pp. 1–11.

See also: Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Follow-up to the multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, Proposal for a Decision of the European Parliament and of the Council amending Decision No 276/1999/EC adopting a Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, doc. n. COM 2002 152, 22 March 2002. Available at <http://www.saferinternet.org/funding/legislation.asp>.

A) SELF-REGULATION INITIATIVES DEVELOPED BY INTERNET SERVICE PROVIDER ASSOCIATIONS

8.4 EU GUIDELINES PERTAINING TO ISPAS IN RELATION TO CHILD PORNOGRAPHY ON THE INTERNET

Internet Self-regulation in the area of child pornography has several distinct aims, which include:

- preventing profit from and dissemination of child pornography,
- preventing the exposure of children to illegal and harmful content, and
- preventing them from being contacted by sexual exploiters and/or abusers.

The central role of codes of conduct in achieving these results is underlined by the EU Council Recommendation on the Protection of Minors and Human Dignity (1998, 7 October).⁴¹ In particular the Recommendation emphasises that 'with full respect for the relevant regulatory frameworks at national and Community level, greater self-regulation by operators should contribute to the *rapid* implementation of *concrete solutions* to the problems of the protection of minors and human dignity'. It is clear that in order to achieve these results, a code of conduct should possess certain features. Although not binding in nature, the Recommendation itself also includes several guidelines for the development of codes of conduct.

More specific is the 'ISPA code review'⁴² completed under the Oxford University IAPCODE Project. It highlights five elements that should be addressed when drafting a code of conduct:⁴³

- the code should be grounded in existing legislation;
- the code must be open to both members and end-users;
- the code should deal with issues such as data protection, privacy, bulk e-mail, and (to a limited extent) information regarding business;
- the code should deal with the sensitive issues of protecting minors from harmful content and regulate hate speech;
- the code should regulate enforcement and sanctions.

According to Council of Europe research on codes of conduct,⁴⁴ an analysis of self-regulatory measures to fight illegal content on the Internet should encompass three areas:

- control of Internet Provider activities;
- protection of users;
- measures to bring together the various actors involved in content regulation.

⁴¹ Council Recommendation of 24 September 1998 on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, doc. 98/560/EC, published on the Official Journal L 270/48 of 7 October 1998.

⁴² The ISPA code review assesses the codes of eight European Union member states (Austria, Belgium, Germany, France, Ireland, Italy, the Netherlands, and the United Kingdom), as well as the codes of Norway, Australia and Canada.

⁴³ Oxford University (2001), *ISPA Code review*. Available at <http://www.selfregulation.info>.

⁴⁴ The research findings are available at http://www.coe.int/T/e/human_rights/.

Based on the wording of the EU provisions, the Council of Europe research and the results from the IAPCODE Project, a set of guidelines to evaluate codes of conduct adopted by national Associations of Internet Service Providers was created. The guidelines are as follows:

1. Existence of measures concerning 'illegal activity'.

The codes of conduct should specifically mention that no illegal material should circulate on the Internet and that ISPs will take reasonable steps to ensure that it is removed.

2. Existence of provisions on 'notice and take down procedures'.

Internet Service Providers hosting content should be obliged to remove illegal content when users, Internet hotlines or law enforcement authorities inform them that such content exists.

3. Existence of provisions to regulate cooperation with law enforcement agencies and third parties.

Internet Service Providers should be encouraged to actively cooperate with law enforcement agencies. They are requested to allow illegal content to be removed from the Internet and to make it possible to freeze evidence in urgent cases as well as to permit other measures aimed at tracing the original posters of illegal material to be taken.

4. Existence of information regarding tools and services supplied to users to facilitate parental controls (i.e. filtering systems).

The codes of conduct should contain mention of filtering technology available to users to facilitate parental control. Parents, teachers and others exercising control in this area should be assisted by easy-to-use and flexible tools in order to enable minors to access Internet services, even when unsupervised, without running risks.

5. Existence of rules on the management of complaints about breaches of the code.

The objective is to promote the effective management of complaints about content that does not comply with the rules on the protection of minors and/or violates the code of conduct.

6. Existence of sanctions for violations of the code of conduct.

The credibility and the effectiveness of the code of conduct should be strengthened, by providing dissuasive measures that are proportionate to the nature of the violations (i.e. suspension of membership or the publication of violations of codes of conduct)

7. Existence of provisions regarding review and amendment of the code of conduct.

A provision should be included that allows for a periodic review and amendment of the code of conduct in order to consider changes in legislation or technological developments.

8. Existence of provisions regarding data protection and privacy.

If information concerning reporters of suspect material is stored, it is important that measures exist to protect their personal data to restrict access to such

information by making it available only on the request of authorities in specified cases.

8.5 MAPPING ISPAS CODES OF CONDUCT

In order to understand what preventive measures have EU Member States enacted in order to fight child pornography on the Internet, a mapping of the codes of conduct adopted by National Internet Service Providers Associations (ISPAs) was carried out. What has been investigated was the presence or absence in existing codes of conduct of each of the guidelines previously outlined.

Before entering into detail and describing the findings, a brief introductory overview of the existing European framework in the field of ISPAs may be useful for understanding the findings themselves. The first aspect to point out is the fact that the validity of a code of conduct is connected to the capability of its promoters to enforce it among the association's members. Moreover, the association enforcing the code should be representative of a large part of the Internet Industry: this will allow the behaviours of key Internet players to be controlled. In this sense, ISPAs could be viewed as Internet gatekeepers.

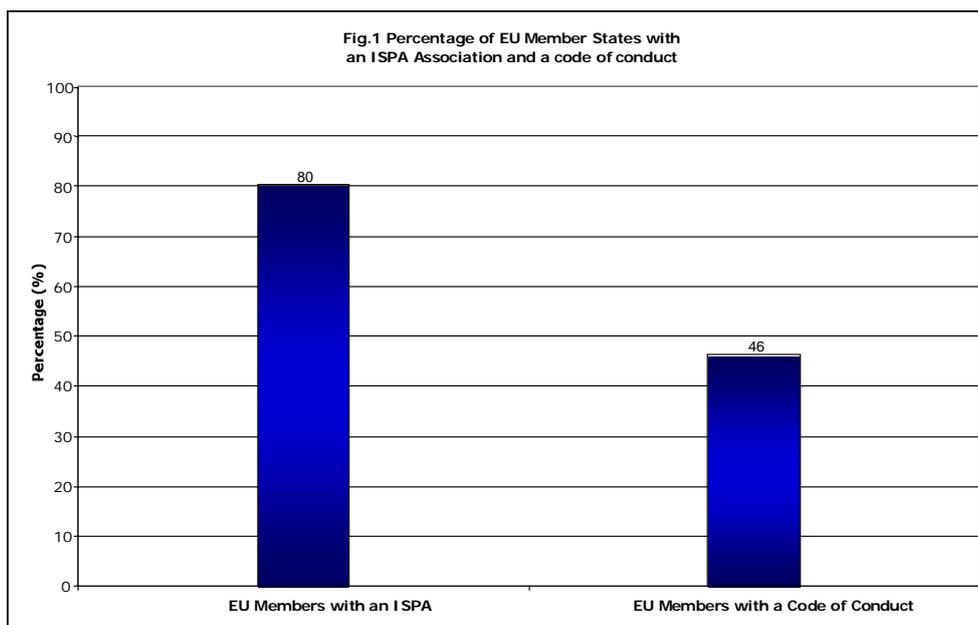
Although the research has focused on ISPAs, it is important to emphasise that the associations contacted were often involved in different kinds of businesses including Internet connectivity. The members of an ISPA may provide one or more of the following services:

- content providers: providers supplying their own content on the Internet;
- access providers: providers supplying access to the Internet for Internet users;
- host providers: providers offering storage space for outside Internet content;
- backbone providers: providers offering international Internet connections.

Some ISPAs also encourage the participation of stakeholders outside the business sectors, such as hotlines, Internet Users Associations, etc.

ISPAs are widespread, though the role they can play as representatives of the entire sector really depends on the each country. For instance, 3 out of 15 countries do not have an ISP association (Greece, Sweden, Finland) while the remainder often have several self-regulatory bodies created with the intent of producing a larger framework for the whole media industry (i.e. Germany, Spain, Portugal, Italy). For the purpose of this research, where more than one association covering ISP related issues was present in a country, only one was chosen. The association selected was always the one most closely involved with the Internet Provider Industry.

It must be emphasised that the existence of an ISPA or similar organisation does not always ensure the existence of a code of conduct. In fact, although some associations were set up years ago, only a few have established a code of conduct: 7 out of 15 associations do not have a code of conduct (Denmark, Finland, Greece, Luxembourg, Portugal, Spain, and Sweden). This high number of ISPAs without a code of conduct (44%) has clearly affected the completeness of this analysis (Figure 1). However, when contacted, the associations without a code of conduct stated that such a document was being developed or already in the process of being released.



When carrying out an analysis of different countries the first obstacle is the language. Few organisations provide their code of conduct in more than one language. Therefore, when it was possible official translations provided by the IAPCODE Project were used. Other codes were read and analysed in their original language.⁴⁵

Before analysing each guideline in detail, it must be noted that the level of completeness of each code of conduct varies according to each ISPA. Some codes were well structured and in many instances had been developed in cooperation with national authorities and law enforcement units. In other cases, the code resembled a minimal set of guidelines and the boundary between a code of conduct and suggestions for best practice was vague. Hence, codes of conducts within the EU Member States range from codes established as a ‘lowest common denominator’ between the parties concerned, to codes defining a concrete set of preventative measures to control criminal behaviour on the Internet.

Complete information on each country’s ISPA organization and code of conduct is summarised in a series of synoptic tables, which are available in Chapter 14, Annex 3. The following are the main findings of the mapping of each guideline:

1. Existence of measures concerning ‘illegal activity’

General references to illegal activities are contained in most codes of conduct though their extension is variable. Illegal activities are referred to as hate speech, child pornography and contents that harm human dignity. In some cases unlawful trading, illegal transaction or anything that could be a crime or infringement are also considered illegal activities. The most common way of defining the set of behaviours banned by the codes is through a direct reference to national criminal law.

2. Existence of provisions on ‘notice and take down procedures’

⁴⁵ The German code of conducts was read and analysed in German.

Notice and take down procedures is an issue covered by all the codes of conduct, though procedures might be very different. Hotline associations frequently receive requests for removal of illicit websites. Where technically and economically feasible, the advice of the take down procedure is posted on the website for one calendar month.

3. Existence of provisions to regulate cooperation with law enforcement agencies and third parties

ISPA members are generally invited to assist law enforcement agencies immediately when necessary, in every way possible and according to the means and resources available to them. Sometimes the cooperation also involves hotlines or special national centres dedicated to the fight against child pornography.

4. Existence of information on tools and services supplied to users to facilitate parental controls (i.e. filtering systems)

Few codes contain references to filtering systems and content rating. ISPA members are generally invited to make their customers aware about the usage and availability of tools that may assist them to filter Internet content. Rating or labelling systems are even less widespread. Various national bodies that are frequently associated to the Internet Content Rating for Europe (INCORE) initiatives often manage Website rating.⁴⁶

5. Existence of rules on the management of complaints for breach of the code

Complaint procedures usually begin with a written complaint (e-mail, fax or letter). A few associations also receive complaints by phone. These reports are then followed by an investigation into the reliability of the complaint. The investigation ends with a judgment that may lead to sanctions. This procedure takes 2-3 weeks on average. In some codes of conduct, the course of actions is described in detail and it is composed of several phases before the judgement is made.

6. Existence of sanctions for violations of the codes of conduct

Sanctions are always included in codes of conducts. They vary from an oral warning to termination of membership depending on the seriousness of the case and the frequency of the non-observance. Usually the scale of sanctions starts with an oral warning and then progresses with a written warning, temporary suspension and termination of the affiliation. The sanctions can be made public through an announcement on a website.

7. Existence of provisions regarding review and amendment of the code of conduct

Only a few codes of conduct do not contain any rules on the review and updating of the code of conduct. Amendments can be made when a new regulation is implemented and/or remarks on the code are made by the members of the organization.

8. Existence of provisions regarding data protection and privacy

ISPA members are generally advised to comply with national and EU laws on privacy and data protection.

⁴⁶ INCORE is a project aimed at setting up a system to describe web-site content. The project is funded by the European Commission under its Action Plan to Promote Safer Use of the Internet.

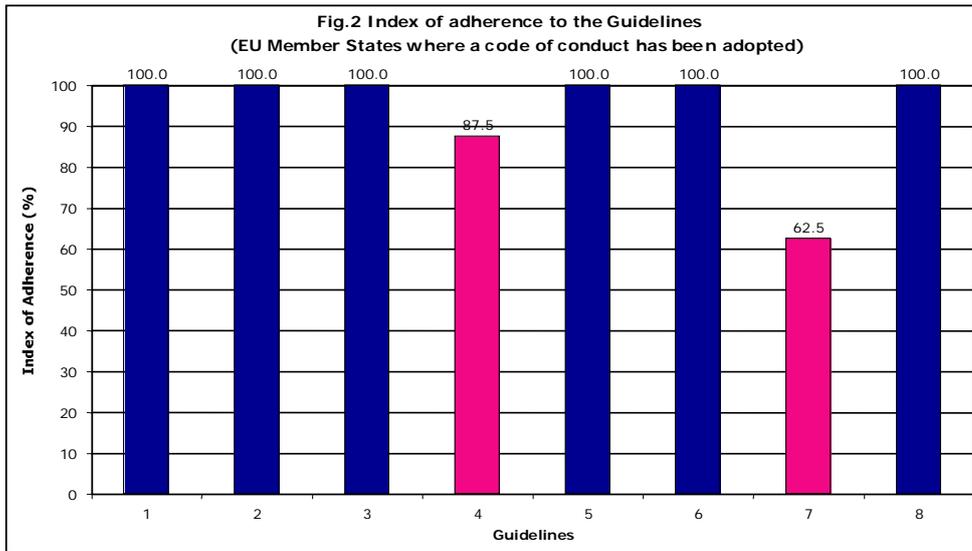
8.6 EVALUATING THE LEVEL OF ADHERENCE TO EU GUIDELINES OF ISPAS CODES OF CONDUCT IN EU MEMBER STATES

This section presents the findings from the evaluation of the level of adherence of ISPAs codes of conduct in EU Member States to the guidelines outlined. This result was achieved by means of an Index of Adherence, elaborated and calculated by using the qualitative information collected for the mapping of existing codes of conduct.

The Index was calculated for each EU Member State and represents, on a scale from 0 to 100, the level of adherence of EU Member States to each guideline against child pornography on the Internet. The higher the Index, the more closely the EU Member State adheres to the guidelines suggested. The higher this Index, the higher the adherence of EU Member States to EU guidelines against child pornography on the Internet.

Where established (8 countries), the codes of conduct seem to completely respect the EU guidelines when dealing with subjects such as protection of minors and procedures concerning complaints (Figure 2). These results are clearly affected by the fact that, at the time of the mapping, to our knowledge, no codes of conduct have been enacted by ISPAs in seven EU Member States (Denmark, Finland, Greece, Luxembourg, Portugal, Spain, and Sweden).

Figure 2 shows the Index of Adherence of EU Member States to the EU Guidelines.



Highest level of adherence:

Guideline n. 1 (Existence of measures concerning 'illegal activity'), guideline n. 2 (Existence of provisions on 'notice and take down procedures'), guideline n. 3 (Existence of provisions to regulate cooperation with law enforcement agencies and third parties), guideline n. 5 (Existence of rules on the management of complaints for breach of the code), guideline n. 6 (Existence of sanctions for violations of the codes of conduct) and guideline n. 8 (Existence of provisions regarding data protection and privacy) – Index of Adherence 100.

Lowest level of adherence:

Guideline n.4 (Existence of provisions on tools and services supplied to users to facilitate parental controls – i.e. filtering systems) – Index of Adherence 87.5, guideline n. 7 (Existence of provisions regarding review and amendment of the code of conduct) – Index of Adherence 62.5.

As shown in the figure above, the two guidelines that scored the lowest level of adherence are n. 4 (tools and service to facilitate parental control) and n.7 (provisions on the code review). These two provisions are the essential parts of a complete code of conduct and their absence may affect the code's comprehensiveness.

Concerning guideline n.4, the presence of statements on filtering systems and content rating shows a willingness to provide concrete help to parents, teachers and other caretakers to help prevent access to unsuitable content. Although existing filtering and rating systems are quite rudimentary and users cannot be sure that the content will be accurately rated and/or blocked,⁴⁷ national ISPAs should provide their consumers with up-to-date information. Hence, provisions on this issue should be inserted in the list of mandatory actions that ISPA members should take.

The lack of provisions regarding amendments and reviewing, however, raises more concerns. Considering how quickly the Internet and its regulation change, a code review process is fundamental. A code that does not reflect the most recent innovations, whether legislative or technological, runs the risk of being an ineffective tool. Self-regulation is not only based on the development and implementation of a code of conduct but also on its administration and maintenance: these two tasks are essential to achieve compliance with laws and industry best practice. However, the validity of such concerns can only be proven through a process of evaluation of the effectiveness of codes of conduct.

⁴⁷ For additional information see Area of Intervention D (Technological measures).

8.7 EVALUATING THE EFFECTIVENESS OF CODES OF CONDUCT

Effective codes of conduct for ISPs could bring substantial benefits to the fight against child pornography on the Internet. Indeed, they have the potential to prevent the distribution of child pornography and the development of abuser rings on the Internet. This explains why part of this research is devoted to the evaluation of the effectiveness of existing codes of conduct.

This evaluation was carried out in three different areas:

1. Structure of the code of conducts, where the following factors were analysed:
 - effectiveness of the 'illegal activities' definition given in each code;
 - effectiveness of complaint procedures and number of complaints processed by the association;
 - type and number of sanctions imposed on ISPA members;
 - frequency and number of reviews and updates of the code of conduct.
2. Prevention and control, where, the preventative measures implemented by ISPAs members to tackle child pornography on the Internet were analysed, i.e.:
 - effectiveness of filtering systems;
 - effectiveness of content rating systems;
 - effectiveness of measures to reduce the anonymity of Internet users;
 - effectiveness of legal provisions making Internet Service Providers liable for child pornography material distributed through their services.
3. Cooperation with law enforcement agencies, where the effectiveness of cooperation between law enforcement agencies and ISPs in order to tackle child pornography on the Internet was assessed. In particular, the following factors were examined:
 - effectiveness of mechanisms for reporting child pornography material to law enforcement and number of reports;
 - effectiveness of cooperation between ISPs and law enforcement and number of investigations carried out;
 - effectiveness of provisions related to the retention of traffic and content data;
 - effectiveness of a common platform established with law enforcement agencies to tackle child pornography on the Internet.

The results of the evaluation are given below, area per area.

Structure of the code of conducts

The definition of 'illegal activities' adopted in the codes was evaluated positively in all the three cases (2 answers were 'very effective' and 1 'effective'). As shown by the mapping, these definitions are often linked to national laws on child pornography and/or other harmful content. In order to maintain such a high level of effectiveness it is vital that the code is updated in accordance with new the national and EU regulations that will be issued soon. Indeed, all the respondents declared that they have already reviewed their codes (or are currently doing the

review) since its adoption. The frequency of updating was evaluated as 'adequate' by all those surveyed.

Within the measures to prevent child pornography, the hotlines established to report child pornography are considered the most effective. Where established, the child pornography reporting lines were considered effective and are often managed in cooperation with law enforcement agencies and national hotlines. However, as noted by one of the respondents, where the reporting procedures are not processed automatically using electronic forwarding, this entails a cost that not all ISPA are willing to incur. Once a report reaches the ISPs, the procedure to withdraw the illegal material from the Internet is considered as 'very effective' by all the respondents.

The rules to manage complaints for breaches of the code of conduct were evaluated positively (all the respondents considered them as 'effective' or 'very effective'). Of the associations that answered the questionnaire, 2 out of 3 have established a set of sanctions in the event of violations. However, it should be pointed out that none of these associations has ever inflicted any sanctions on its members so these measures cannot be judged.

Prevention and control

Concerning prevention and control measures, the evaluation of filtering systems and content rating mechanisms can be considered negative. Only two of those interviewed answered the questions on filtering and content rating and both agreed on the ineffectiveness of these measures. These answers are consistent with the results of the mapping, where guideline number 4 – existence of provisions on tools and services supplied to users to facilitate parental controls – scored the lowest. The results of the mapping show that few codes of conduct contain references to filtering systems and content rating and ISPA members are generally invited to make their customers aware of the usage and availability of such tools without providing more in-depth information.

Where ISPs have a duty to clearly identify their customers in order to reduce the level of anonymity, such provisions were judged as 'quite effective' (2 respondents). The provision that compels ISPs to disclose subscriber information to law enforcement agencies during an investigation is unanimously evaluated as 'very effective'.

Cooperation with Law Enforcement Agencies

All the respondents evaluate cooperation with law enforcement as 'very effective'. However, as stated above, no associations have defined a common platform for cooperation with law enforcement agencies. Hence, the exchange of intelligence as well as the procedures to help police carry out investigations is not well defined.

Only in one country does the law compel ISPs to advise competent authorities about child pornography material that is distributed by exploiting their facilities. Where the provision is present, it is considered 'effective'. Only two countries have provisions compelling ISPs to retain traffic data for law enforcement investigation purposes. Regarding content data retention, only one country has a similar regulation. However, where they exist, both provisions on traffic and content data retention were evaluated as 'effective'.

8.8 CONCLUSIONS

Effective voluntary codes of conduct carry substantial benefits for governments, the industry and consumers when they are implemented to enforce compliance to control criminal phenomena such as child pornography on the Internet. A huge obstacle to promoting such an approach is its sustainability. Self-regulation is often perceived as a competitive disadvantage as it places compliance burdens on businesses without an immediate return on their investment. However, this way of thinking is accurate only when the codes of conduct are ineffective and fail to provide any real benefits to the industry sector.

As emerged from the research, EU ISPAs are at the beginning of creating a good self-regulatory scheme. One cannot avoid the impression of heterogeneity and sometimes incoherence when reading some rules, which leads one to fear that most could remain empty words. As emerged from the mapping activity, it should be acknowledged that the harmonization of the activities between countries should be the objective of future EU initiatives on self-regulation. However, a prerequisite for such a campaign is the presence within each EU Member State of a reliable Internet Industry referee. The first step required is to support the creation of national regulatory bodies that are able to reach a critical number of market participants by including the major players, while striking a balance between commercial and law enforcement interests. National ISPAs could play this role, they should, however, strengthen their position in the countries in which they are not the main body by interacting with the majority of Internet Industry stakeholders. In those countries where they are not present, they should be established; conversely, where more than one ISPA exists, the number should be reduced in order to define a single counterpart within the Industry sector that can act as a representative for all the players.

In spite of the fact that ISPA representatives do not like to be addressed as Internet gatekeepers, it is also true that they could play such a role. When tackling child pornography on the Internet, one can state that the ISPs are similar to banks in the fight against money laundering, as they are an independent party that can easily spot suspect transactions. Nonetheless, market constraints clearly affect an ISP's approach, as they are alarmed about being pushed out of the market by unscrupulous providers outside EU borders. The international nature of the Internet clearly raises concerns about this issue, though these should not prevent the industry from engaging in such activities. While these initiatives may be seen as being contrary to their economic interests in the short term, they will provide a return on the investment in the long term. Moreover, several countries are working on codes of conduct and other initiatives that are more stringent than those in Europe, as the Australian Internet Industry (AII) code demonstrates.⁴⁸ The AII code provides a basis for ongoing cooperation between law enforcement agencies and ISPs in relation to the prevention, detection and investigation of criminal activity perpetrated through the Internet. This code provides a set of procedures for cooperation in order to ensure that all investigative costs and efforts are minimized and equitably divided between the parties involved.

The EU Commission should therefore pursue the harmonization of self-regulatory schemes in all EU Member States as well as provide incoming countries with

⁴⁸ IIA, *Cybercrime code of practice* (2003). Retrieved from [http://www.ii.net.au/cybercrime_code_v2\(cIn\).doc](http://www.ii.net.au/cybercrime_code_v2(cIn).doc)

guidelines and suggestions to develop those schemes. Cooperation between the stakeholders would certainly be enhanced and, at the same time, the quality and number of the initiatives against child pornography would benefit from this improved scenario.

The seminar held in Brussels in January 2004 brought together different expertise from law enforcement, hotline representatives and the Internet industry (mostly ISPA members). The initiative's aim was to discuss the findings of the activities carried out and to develop guidelines to overcome some of the above-mentioned obstacles while defining how an effective self-regulatory scheme should work.

The ISPA membership theme was discussed as a central point in order to develop effective codes of conduct. The fact that several members of national ISPAs are involved in different kinds of businesses entails a higher level of effort when drafting a code that can be applied to all the parties involved. This element, together with the different legal restrictions in force in each EU Member State, discourages the introduction of a code of conduct promoted directly by the EU Commission with the cooperation of various ISPAs. It has been argued that a common code of conduct would not be feasible due to the different levels of development among each of these associations as well as the diverse standards that each of the associations will have created according to their own national legislation.

Although a common EU code of conduct is not considered a viable solution there is still an urgent need to find an alternative path as findings from the mapping activity have disclosed. Participants agreed that a set of common key features should be enacted in order to harmonize the different codes of conduct and enable them to be effective tools to tackle criminal behaviour. For instance, it is vital that a code of conduct includes a review process in order to keep it up-to-date and functional. Although notice and take down procedures operate as reactive measures to child pornography, they should also be considered as key features for a code of conduct and be consistent throughout the EU. Therefore, the involvement of the EU Commission and national government bodies in promoting such harmonization should be encouraged.

Seminar participants rejected the idea of developing a common EU platform for enacting cooperation between ISPs and the law enforcement agencies that carry out investigations. Where not already established, a memorandum of understanding between ISPs and law enforcement agencies would serve to smooth and ease cooperation. Currently, most of the contacts between investigators and ISPs are maintained through informal and personal communications. Each Cyber Crime Unit maintains its own "red line" to contact national ISPs when their help is required. However, this may cause problems to both ISPs, which can be called upon to go further than they are permitted when collecting information, i.e. turn a blind eye to EU rules on personal data protection, as well as law enforcement, which may run the risk of seeing their investigation delayed if their usual contact is not available. It could be useful to develop good protocols for the exchange of information in each country according to its national laws. The agreement signed between the Belgian police forces, the Minister of Justice, the Minister for Telecommunications and the Belgian ISPA could become a template for similar initiatives.⁴⁹

⁴⁹ Seminar communication (16th January, 2004), Yves Goethal, child pornography coordinator, Federal Police Belgium.

As regards cooperation with law enforcement, a standard form for an information request would be valuable to speed up an ISP's activities when retrieving data. While in some countries, such as the United Kingdom, a standard form already exists, most EU members do not have similar tools. The setting up of a single point of contact between ISPs and law enforcement units in order to avoid processing multiple requests, which all involve the same investigation, would also be advisable.⁵⁰ However, the obstacles to developing such initiatives lie in the willingness of ISPs to invest money or find alternative financial support.

Within the context of cooperation between ISPA and law enforcement, the willingness and capability of ISPs to get involved in the fight against child pornography has been widely discussed. ISPs and other Internet related businesses have often been seen as enterprises composed of technicians who cannot be called upon to work on complicated legal topics related to computer crime and child pornography. There are obviously limits to the interventions that can be requested of ISPA Members. Nonetheless, the EU Commission is currently making efforts to bridge this gap. For instance, the RAND Handbook⁵¹ is an easy to use guide that matches technical descriptions of incidents to the legal framework of the country in question and details procedures for working with law enforcement to respond to incidents. Although it has been developed to help Computer Security Incident Response Teams (CSIRTs) meet their challenges, it could also provide Internet businesses with the legal knowledge they need.

Indeed, ISPA members, namely service providers, access providers and content providers, are not called upon to present definitive solutions in the fight against child pornography but to cooperate to reduce crime opportunities. Following crime prevention theories,⁵² ISPA members could be "capable guardians" while helping to reduce the availability of "suitable targets". As suggested, ISPA could work on three different preventative approaches:⁵³

1. Prevent perpetrators, either abusers or child pornography consumers, accessing the necessary technological infrastructures;
2. Prevent people from accessing child pornography already circulating on the Internet;
3. Prevent children from being contacted by abusers thereby helping the development of a safer environment.

With regards to point one, participants were divided on the effectiveness of acceptable user policies that clearly state the user's liability for showing/distributing/exchanging illegal materials. Although, it is clear that such a simple measure cannot prevent criminals from pursuing their goals, they could constitute a barrier for simple viewers. As ISPA representatives pointed out, other key players should be scrutinized when looking at the infrastructures used to exchange child pornography, in particular the mobile phone industry. This industry is becoming the new access provider for the Internet. It is now facing the same

⁵⁰ Seminar communication (16th January, 2004), Michael Rotert, EuroISPA President.

⁵¹ RAND Europe, (2003) Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, retrieved from <http://www.iaac.org.uk/csirt.htm>.

⁵² Clarke, R. (1980) Situational Crime Prevention: Theory and Practice, *British Journal of Criminology*, 20, pag. 136-147. and Cohen, L. and M. Felson. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, 44, pag. 588-08.

⁵³ Seminar communication (16th January, 2004), Thomas Rickert, INHOPE President .

problems ISPs have been coping with for years. As the Internet is about to go mobile, it may be more difficult to prevent or detect crimes. Hence, the fight against child pornography will soon involve more participants.⁵⁴ For instance, search engines should also be closely looked at when dealing with child pornography. Due to their massive archives of Internet web pages and their work as indexers, search engines could help to prevent children from accessing illegal content. In Germany, search engines are requested to work with a Commissioner for youth protection in order to identify which content may not be suitable for underage individuals.

As regards responsibility for accessing illegal content, the main attitude within the Internet industry is to move such responsibility from ISPs to individual users. The results from the questionnaire suggest that content filtering is not useful, demonstrated by the hesitation of ISPs to confirm the utility of filtering software at the ISP level. However, it has been suggested that, as happened with anti-virus software, there could be a market for ISPs providing anti-porn filtering facilities. It should be noted that the market for content filtering systems has not developed at all, as few industries are interested in investing money in such tools, as emerged from the research carried out by Unisys.

Even though ISPA members could provide good gate-keeping services for the Internet, certain content should not be subject to self-regulation schemes for reasons of ethics and democracy. The interpretation of some values cannot be appropriated or usurped by particular interests. As discussed during the seminar, ISPA members cannot be called upon to assess the legitimacy of the content or be the censor of Internet. Conversely, ISPA members should work together to define rules in order to control the access to high-risk services such as chat rooms, peer-to-peer networks and IRC. For instance, strict registration rules for joining IRC services could help in both the identification and traceability of users. Furthermore, national ISPAs could promote the development of common Internet standards. The use of common standards for digital certificates could be an example of how illegal behaviour could be stopped through industry self-regulation. Common standards could be implemented regarding both technological solutions and consumer protection initiatives (i.e. data collection and privacy rights).

⁵⁴ In January 2004, mobile phone operators in the UK announced a joint code of practice for the self-regulation of new forms of content on mobile phones. Mobile operators have signed up to the code designed to facilitate the responsible use of new mobile phone services whilst safeguarding children from unsuitable content on their mobile phones. A copy of the code is available from the website of each of the operators (Orange, O2, T-Mobile, Virgin Mobile, Vodafone and 3).

B) SELF-REGULATION INITIATIVES DEVELOPED BY HOTLINES

8.9 EU GUIDELINES FOR NATIONAL INTERNET HOTLINES

Even though hotlines, as points of contact for receiving reports about suspected child pornography material publicly available on the Internet, are generally mentioned in EU documents, no specific guidelines concerning their organisation and functioning are given directly by EU institutions.

In Decision n. 276/1999/EC of the European Parliament and the Council, commonly known as the Safer Internet Action Plan, it is clearly stated that 'cooperation from the industry in setting up voluntary systems of self-regulation can efficiently limit the flow of illegal content on the Internet.' Furthermore, 'hotline reporting mechanisms which allow users to report content which they consider illegal should be made available to the public. [...] Hotline reporting mechanisms should support and promote measures taken by the Member States; hotline reporting mechanisms should be established in cooperation with the law enforcement authorities of the Member States.'

Furthermore, within its Action line n. 1 the Safer Internet Action Plan strongly emphasised the importance of creating a European network of hotlines, which would allow Internet users to report material they suspect could be child pornography.⁵⁵ The creation of a hotline in all EU Member States should be encouraged, together with mechanisms for the exchange of information between national hotlines and the European network as well as hotlines in third countries. Cooperation between hotlines and law enforcement authorities should also be promoted, by encouraging the exchange of information and experience between the two bodies.

Based on these general elements, and the suggestions gathered during discussions with experts concerning the mapping questionnaire and an analysis of the available literature, a series of guidelines were extrapolated by the researchers. The EU guidelines identified were grouped into the following thematic fields:

1. Minimum standards for operating Internet hotlines and organisation of the hotline.
2. Procedures for handling complaints.
3. Privacy of data.

-

Minimum standards for operating Internet hotlines (thematic field)

Hotlines should be:

Easy to find using a search engine. Hotlines have to be available and users must be made aware of their existence. For this reason, a hotline website needs to be easily traceable on the Internet, so that users can report suspected child pornography material with the least effort possible.

⁵⁵ *Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, Annex 1 to Decision n. 276/1999/EC of the European Parliament and of the Council on 25 January 1999, published in Official Journal L33/6, 6 February 1999, Action line 1, point 1.1.

Involved in awareness initiatives. Even though the primary task of hotlines is to communicate the existence of illegal content circulating on the Internet to law enforcement and the Industry, awareness is a necessary complement to their activities. Their actions as well as the actions of the Industry to implement measures against child pornography on the Internet will bear fruit only if users and potential users are aware of their existence and users are made aware of measures on how to use the Internet safely.

Equipped with mechanisms for receiving complaints operating on a 24-hour/7 days a week basis. Hotlines should be open on a 24-hour/7 days a week basis, in order to allow prompt screening of all incoming reports and a quick procedure to forward them to law enforcement authorities.

Procedures for handling complaints (thematic field)

Existence of simple methods for users to forward complaints. Several methods should be available to access hotlines so that reporters can send their complaints: forms to be compiled online or other means of communications, such as e-mail, fax or telephone. The more numerous and easier the methods available for potential complainants are, the more users will be encouraged to make reports.

Acceptance not only of reports where the complainant is identifiable, but also of anonymous complaints. Reporters may find it preferable to remain anonymous when making a complaint, and might be discouraged from forwarding a complaint, if they have to identify themselves.

If the reported content is located abroad, existence of methods for the exchange of information with the hotline/law enforcement authority in the country where the reported material is located. If the child pornography material is hosted in another country, it is important that methods exist for the immediate forwarding of the complaint to the hotline or the law enforcement authorities of that country.

Protection of hotline staff from any legal action concerning the material they handle by legal provisions or arrangements with law enforcement or other public authorities. Hotline staff should be shielded by a 'safe harbour' provision, from criminal and civil liability encountered when conducting their business. Distribution and, in most EU Member States, possession of child pornography material is in fact illegal, but the tasks of hotline employees include checking the material, tracing its location and reporting it to law enforcement authorities, or other hotlines or ISPs.

Privacy of data (thematic field)

Existence of measures to ensure the protection and to regulate access to personal data concerning reporters: a) personal data on reporters may be stored only after consent has been given, while access to personal data should be limited and reserved b) if a complaint is forwarded to national/foreign authorities, personal details concerning reporters should not be passed on. If information concerning reporters is stored, it is important that measures be provided for the protection of personal data, so that access to such information is limited only to the hotline personnel working on the report and that, in the case of storage, consent is given by the reporter.

8.10 MAPPING THE NATIONAL INTERNET HOTLINES IN EU MEMBER STATES

As stated previously National Internet hotlines provide a central point of contact for the Internet industry, law enforcement and Internet users who become aware of child pornography and other illegal content available on the Internet.⁵⁶ Additionally, they play an important role in Internet governance and, in particular, the prevention of child pornography. In order to enhance their capabilities and resources, it is important to understand and evaluate how the existing framework in EU Member States in the area of Internet hotlines is organised.

The following analysis was made on the basis of the answers given by the thirteen Internet hotlines established in EU Member States which completed the questionnaire sent to them to learn about their structure and methods of operation. Before entering into detail, it is necessary to underline that, for confidentiality reasons, the qualitative information collected for the description of National Internet hotlines in EU Member States has been analysed and reported here in a way that ensures that no hotline can be identified by the text.

A review of Internet hotlines highlights a variety of different approaches to the problem of illegal and harmful use of the Internet. In this context, the structure and background of the organisation running the hotline is very important. Some countries have followed government initiatives to establish organisations connected to government and law enforcement. Others have encouraged a self-regulatory approach by the Industry or industry associations. More recently established hotlines come from the child welfare sector and are particularly proficient in the promotion of safety on the Internet to children.⁵⁷ Six of the hotlines that responded to the questionnaire were established by child welfare and protection organisations, six were created by Internet Industry groups (mainly ISP Associations) and one is a publicly owned institution. As public authorities do not run most hotlines, it is necessary for them to establish links with law enforcement agencies or the relevant ministries. This has been accomplished mainly through cooperation agreements.

Although hotlines could choose to receive reports on any illegal activities they choose, the hotlines that were the subject of this report have directed their activities towards areas of illegal content involving children as victims.⁵⁸ All hotlines within this analysis are competent to receive reports on suspected child pornography material publicly available on the Internet. Additionally, many hotlines deal with other types of illegal material or activity. Eight hotlines handle reports concerning racist or extreme political material, two accept reports regarding obscene adult material and one screens all reports about any Internet content considered illegal by national legislation.

Differences are also to be found in the type of media that hotlines concern themselves with. Importantly, all the hotlines that responded to the questionnaire accept reports of suspected child pornography available on the World Wide Web. All but one hotline cover newsgroups, six hotlines deal with Internet Relay Chats, four

⁵⁶ It should be mentioned that in most EU Member States, law enforcement agencies have also established contact points, for instance in Austria, Belgium, Denmark, Italy, Portugal, Sweden.

⁵⁷ INHOPE Association of Internet Hotline Providers in Europe, *First Report*, INHOPE, May 2002, available online at www.inhope.org, p. 5.

⁵⁸ ICRI K.U. Leuven, *Legal issues with regard to the activities of hotlines in the battle against child pornography on the Internet*, Belgium, June 2001, p. 13.

with e-mails and two hotlines cover peer to peer (file sharing). With regards their geographical scope of competence, all hotlines focus on all suspected child pornography material circulating in the above-mentioned means of communication and available in their country, irrespective of where it is hosted.

One aspect of particular relevance for Internet hotlines is the transparency of the hotline. Their website needs to have a clear-cut structure, allowing users to find all necessary information regarding the procedural and legal consequences of contacting the hotline and the way in which their report will be handled. Some hotlines have chosen to have a very simple web page, usually containing some information and instructions to the reporter on what to include in their complaint. Others have a more sophisticated website, which also contains information on national legislation against child pornography, links to other hotlines and child welfare and protection organisations, and a report sheet to be filled in online. Recognising the importance of this aspect, nine of the thirteen hotlines analysed have used the services of a professional web designer in the creation of their website.

Availability is another important issue. Hotlines have to be 'visible', so that users are made aware of their existence. For this reason, a hotline website needs to be easily traceable on the Internet using a search engine, so that users can report suspected child pornography material with the least effort possible. All the hotlines under consideration use a variety of different means to make users aware of their existence. Examples are the existence of active banners on the main portals and children community sites, as well as logos appearing on ISPs and content providers. Furthermore, eight hotlines have produced leaflets that publicise their existence and activities. Three have also chosen to have their activity publicised through television, radio or newspapers. In one interesting case, a hotline used the cooperation of a public relations agency.

These means of communication are often used by hotlines to promote awareness of the safe use of the Internet. Even though the primary task of hotlines is to communicate the existence of illegal content circulating on the Internet to law enforcement and the Industry, awareness is in fact a necessary complement to the activity of hotlines. Consequently, only three hotlines reported limiting their advertising activities to promoting the hotline itself, while the others are also involved in more general awareness campaigns, often with the cooperation of the funding institutions.

Hotlines also have to consider the relevance of one last element, the writing and publication of periodic reports. This point is also important when discussing the visibility of the hotline. Eight hotlines publish such reports, normally on an annual basis, but not all of them are available online or, if they are, not all are in English.

All hotlines have permanent full-time or part-time staff. Hotline employees appear to have a variety of different skills and backgrounds. On average, hotlines employ three to four persons (with the notable exception of one hotline reporting only one person working and another reporting to have 10 employees). Most hotlines are staffed with full-time employees and they come from variety of different backgrounds. Most are lawyers and computer or Internet industry technicians. Some are social workers or have experience in child welfare and education. Less common seems to be the presence of former police officers, mentioned by one hotline, as well as criminologists noted by another.

In order to harmonise their backgrounds and acquire the skills necessary to do their job, hotline employees undergo a period of training. In most hotlines (all but three)

initial training is provided, mostly done on-the-job, and it concerns legal issues as well as practical aspects related to recognising images of child abuse. In some instances, the training involves visits to other hotlines or training provided by law enforcement agencies.

One of the requirements, set out by EU documents, regards their availability on a 24-hour/7 days a week basis. This availability allows for the prompt screening of all incoming reports and a quick procedure to forward them to law enforcement authorities, all but one of the hotlines reports being continuously active.

A variety of means is at the user's disposal to send their report. The more numerous and easier the methods available for potential complainants, the more users will be encouraged to report. On the website of twelve hotlines, report sheets are available and can be compiled online. This mode of reporting in addition to e-mail (available on 12 hotline web sites), are the ones preferred by hotlines, as it allows the reporter to be guided through the information required and allows quick and effective screening of the suspected material by the hotline staff. Furthermore, nine hotlines also receive complaints via fax, and seven by telephone. Only five hotlines, however, provide instructions to users regarding what content their report should have, in case they decided not to use the report sheet, or if this was temporarily unavailable.

A user's decision to make a complaint might depend on whether anonymous complaints are permitted. Reporters may in fact find it preferable to remain anonymous when making a complaint, and might be discouraged from doing so if they have to identify themselves. In response to this need, all the hotlines but one report accepting both identifiable and anonymous complaints.

Once a complaint is received, a predetermined response procedure should be started that processes the report to identify the source of the content and to evaluate whether or not the content is illegal child pornography material. All but one hotline processes complaints according to formal criteria (mainly legal standards, i.e. national child pornography legislation, and good practice) in order to determine its legality. This preliminary check is very useful to law enforcement agencies as well as Internet Providers, because it minimises 'overreaction', thereby protecting freedom of expression.⁵⁹ When hotline employees determine the potential illegality of the material, they try to trace its location to ascertain whether it is located within their country or not. A decision is then made as to whether or not to forward the message to partner hotlines, law enforcement agencies or Internet providers.

In those instances where the material is illegal by their national standards, reports are always forwarded to national law enforcement agencies for further investigation. The majority of hotlines also advise the Internet Service Provider of the existence of potentially illegal material being distributed through them. In some cases, the original poster is advised to remove the potentially illegal content. A single hotline, in other words, may employ one or more of these approaches for each report. Thanks to the collaboration between hotlines and ISPs (which, in many cases, are the hotline's funding institution), contacting content or service providers by hotlines can be achieved far more quickly than by law enforcement.⁶⁰

⁵⁹ M. Machill, A. Rewer, *Internet-Hotlines. Evaluation and self-regulation of Internet content*, Verlag Beltersmann Stiftung, Germany, 2001, p. 69.

⁶⁰ *Ibid*, p. 58.

If the reported content is located abroad, all hotlines forward the complaint to a partner hotline in the country concerned. Two hotlines forward reports to the law enforcement agency of that country. In case the hotline cannot verify whether the complaint actually regards illegal material, the report is forwarded to national law enforcement authorities for their intelligence gathering. The only exception to this procedure applies to one hotline, which does not evaluate reported content, but merely carries out a formal check and forwards the complaint directly to its national law enforcement agencies, where the material is checked in order to determine its illegality.

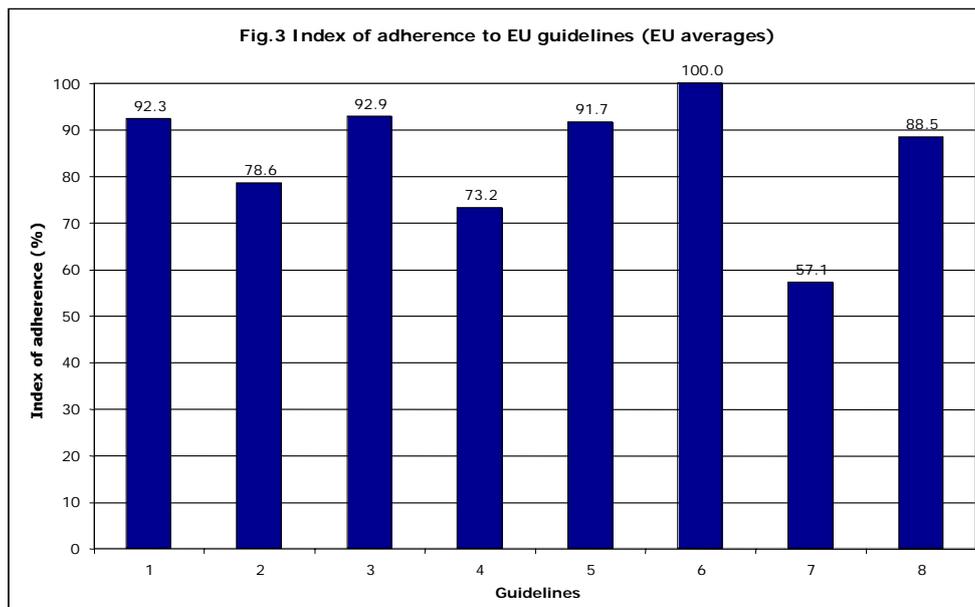
Dealing with potentially illegal material might pose a legal problem for hotline staff who may commit a criminal offence by possessing child pornography material (in the EU Member States where possession is illegal) and for distributing it, where the complaint is forwarded to partner hotlines abroad. It is therefore important that hotline employees be protected from any legal action concerning the material that they handle. It is an INHOPE requirement that members are not entitled to store or forward illegal material. Normally appropriate legal provisions (e.g., 'safe harbour' provisions) or arrangements with law enforcement or other public authorities ensure the protection of hotlines staff. Only half of the hotlines reported being protected by this 'safe harbour' provision.

Finally, one aspect that hotlines need to consider, if anonymous communications are not permitted, is the protection of personal data concerning complainants. Reporters should be sufficiently guaranteed that their identity will not be revealed, this could be done by legal means and approved technical means as well as through legal encryption, etc.⁶¹ Nine hotlines report storing such personal data. In this case, four of them ask for the reporter's consent, who, as we have already seen, in the vast majority of cases has the option of remaining anonymous. Personal data, however, can only be accessed by hotline staff working on the report; in no case but one, are personal details concerning reporters passed on to partner hotlines when the complaint is sent abroad, and then only with written consent by the reporter.

8.11 EVALUATING THE LEVEL OF ADHERENCE TO EU GUIDELINES OF THE SELF-REGULATION INITIATIVES DEVELOPED BY NATIONAL INTERNET HOTLINES IN EU MEMBER STATES

As in the previous section on ISPA initiatives, an Index of adherence, from 0 to 100, was calculated for each EU Member State and represents the level of observance of hotlines in the EU Member States to each identified guideline against child pornography on the Internet. Similarly, the higher the Index, the more closely the EU Member State adheres to the guidelines suggested.

⁶¹ ICRI K.U. Leuven, *Legal issues with regard to the activities of hotlines in the battle against child pornography on the Internet*, cit., p. 21.



Highest level of adherence:

Guideline n. 6 (If the reported content is located abroad, existence of methods for the exchange of information with the concerned hotline/law enforcement authority where the reported material is located) – Index of Adherence 100.0;

Guideline n. 3 (Existence of mechanisms for receiving complaints operating on a 24-hour/7 days a week basis) – Index of Adherence 92.3;

Guideline n. 1 (Easy to find using a search engine) – Index of Adherence 91.7;

Guideline n. 5 (Acceptance not only of reports where the complainant is identifiable, but also of anonymous complaints) – Index of Adherence 90.9.

Lowest level of adherence:

Guideline n. 7 (Protection of the hotline staff from any legal action concerning the material that they handle by legal provisions or arrangements with law enforcement or other public authorities) – Index of Adherence 61.5.

The analysis of the level of adherence of Internet hotlines to the guidelines against child pornography on the Internet shows a very high level of adherence to the majority of guidelines identified. This is probably because a network of hotlines was established through the Association INHOPE, which includes the majority of hotlines existing in EU Member States and whose membership requires the establishment of minimum standards regarding both structure and operational rules.

As shown in the graph, National Internet hotlines in the European Union show Indexes of Adherence higher than 70.0 for all guidelines, with the exception of guideline n. 7, which refers to the existence of measures to protect hotline staff from any legal action concerning the material that they handle by legal provisions or arrangements with law enforcement or other public authorities. The Index of Adherence to this guideline is 61.5, showing that a little more than half of the EU Member States have enacted this 'safe harbour' provision. Member States who have still not enacted such a provision should consider doing so.

8.12 EVALUATING NATIONAL INTERNET HOTLINES IN EU MEMBER STATES

As noted in the mapping section, hotlines provide an obvious and necessary service to Internet users as well as to other stakeholders interested in combating child pornography. Nearly all the hotlines in Europe are part of, or are attempting to be part of, the INHOPE network, which plays an essential role in harmonization and facilitates cooperation between the many different hotlines. Given this relationship between the hotlines and the larger INHOPE body, it seemed prudent to evaluate not only the work of the individual hotlines but also that of the INHOPE network. As stated previously, contact was made with this organization as well as the different hotlines in order to map the services that are provided via hotlines. In order to evaluate these services effectively the collaboration of INHOPE is essential. In theory, the best evaluations are ongoing and occur at many different stages of growth in order to address potential problems in the early stages as well as evaluate the measures taken to address those issues.

INHOPE is a relatively new network that is still struggling for funding and effective cooperation between its members. These two features have created difficulties for the second part of this project, in that INHOPE is currently carrying out self-evaluations and are therefore reticent to have an outside body evaluate the functioning of their hotlines. As nearly all hotlines within Europe are part of the network, or wish to be part of the network, without the collaboration of INHOPE, the ability to gain access to potentially confidential information is severely limited. Furthermore, to receive the most complete evaluation it would be necessary to ask many different stakeholders to evaluate the functioning and effectiveness of hotlines.

Considering the 'newness' of the INHOPE network and the hotlines themselves, data and experience are not yet available in sufficient quantities to conduct a thorough and complete evaluation. This, however, will not always be the case. Evaluations can and should be conducted on hotlines and the INHOPE network in order to improve their functioning as well as to highlight their importance in order to gain increased funding and the support of key stakeholders. Therefore, it was deemed important to produce a questionnaire that could serve as a model for future evaluations⁶². This questionnaire was created by reviewing the work previously completed in the mapping section, the annual report of INHOPE, its mission statement as well as the available reports produced by national hotlines. This questionnaire served as a roadmap for the following evaluation, meaning that the questions (when possible) were answered using available secondary sources.

Although the information may be limited, INHOPE has recently written a first year report, which covers many of the areas that would be included in an evaluation. Most importantly, as stated above, it provides a guide by which an evaluation of the materials available could be created. This therefore enables us to report on what has been done as well as what needs to be done in order to make this important service more effective in achieving its goals.

⁶² The evaluation questionnaire is available in Chapter 14, Annex 2.

8.12.1 Safer Internet Action Plan and INHOPE

One of the goals of the Safer Internet Action Plan was to create an effective system enabling European internet users to report what they believe to be illegal content. This goal naturally creates the question what is an 'effective' system.⁶³ This could be answered by saying that an effective system is one that is widely recognized and known by the public. Further, the system offers a variety of ways to report the content in question to a trusted body. This body then acts on the information provided in a predictable and dependable way. This is the best starting place to evaluate the effectiveness of hotlines, and by default, INHOPE, in reaching the goals they have set for themselves.

Many of the points previously mentioned were reviewed in the mapping section. The INHOPE first year report, provided figures for three of their members regarding the average number of reports received per month. These numbers ranged from 100 to 600 per month suggesting that there is great discrepancy in regards to the visibility of hotlines throughout Europe. The following caveat needs to be provided, however, the number of Internet users may be different in each country so these statistics should be standardized to reflect the number of reports per 100,000 Internet users in order to have comparisons across countries. Furthermore, there must be a commonly agreed upon definition for 'Internet user.'

Within the mapping section, it was determined that all of the hotlines provide several different ways of reporting illegal content. However, it seems that the preference is towards web-based reporting or emails. In some cases, other forms of reporting are discouraged. In trying to create an effective system for European Internet users to report child pornography, all modes of reporting should be encouraged and available. This could be of particular importance to people who do not feel confident in their computer skills and wish to discuss what they or someone they care for has seen on the Internet. During the INHOPE conference in Berlin – *The Internet in 2004: Safe or Just Safer?* – several people discussed the importance of having the option telephoning for guidance and help as opposed to the simple submission of a report via a website.⁶⁴ Considering the importance of hotlines in creating this network, discouraging reports via telephone detracts from the relationship that hotlines seek to have with the public. Hotlines are an effective way of providing help to the community and receiving reports about potentially illegal material; therefore, they cannot limit their contacts to a web-based environment.

As the goal set out within the Safer Internet Action plan is to create a network of reporting, knowledge of each hotline's existence is a prerequisite. This was also reviewed in the mapping section and it was determined that hotlines use many different ways to reach the public and inform of them of the services available (e.g.

⁶³ Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM(2000) 890 Final

⁶⁴ In November 2003 INHOPE hosted a conference in a Berlin entitled *The Internet in 2004: Safe or Just Safer* which sought to discuss the existing relationships between hotlines, ISPs and law enforcement. There were several break out discussion which discussed many of the themes explored in this report (e.g. *Internet Technology, Self Regulation and Defence Strategies; Criminal activity, Effective Investigation and Prosecution; Internet Safety Education – Are we reaching the Key Audiences?*) One of the speakers, Anne Collier of Net Family News based in the USA stressed the importance of having several venues available to assist parents who may be fearful of technology.

banner ads and logos on various websites, leaflets, television, radio). In addition to these public relations activities, many hotlines have participated in conferences where they are able to collaborate with other stakeholders and disseminate information about their activities. One of the only ways to measure the 'effectiveness' of such awareness campaigns is through before and after measurements of the reports received. As this data is not available publicly or may not yet be gathered, it is crucial that this type of measurement be instituted in order to determine the efficacy of such actions. One methodology to measure this would be to map the awareness initiatives over the course of one year and compare those initiatives to increases or decreases in the number of reports received. As not all hotlines use the same awareness techniques, it provides a natural control for the effectiveness of one campaign compared to another.

The hotlines are clearly aware of the importance of providing multiple ways of reporting as well as the need to reach key audiences in many different formats. The creativity of the hotlines to reach parents, teachers, and children is demonstrated through their websites and the activities that are mentioned in the first report produced by INHOPE. In light of the fact that INHOPE (and its associated hotlines) are, in essence, social service providers who historically receive less funding, what they have accomplished in the three years since their inception is remarkable. They have met the fundamental goal of creating a system of reporting child pornography; however, much work remains in order to raise awareness and build a trust relationship with the public. Hotlines are, in many ways, the first line of defence and this role requires flexibility and the ability to respond quickly to the needs of the public. This can only be accomplished with sufficient funding, and support of the larger stakeholder groups.

8.12.2 INHOPE

The mission statement of INHOPE is to 'facilitate and coordinate the work of European hotlines in responding to illegal use and content on the Internet.' This goal is reached through a series of six objectives. Following each objective the INHOPE Association identifies how they intend to accomplish it. This information serves as the basis for the questions that form the evaluation. The objectives are as follows:

- To facilitate the exchange of expertise
- To facilitate the exchange of reports
- To interface with initiatives outside of the EU
- To educate and inform policymakers, particularly at the international level
- To promote awareness of the INHOPE Association and the Individual hotlines
- To ensure that the central administration of the hotline network is provided in an efficient, transparent and accountable manner

As the evaluation of INHOPE and the member hotlines has been largely completed by doing desk research and a review of secondary documentation, each of these goals are not discussed individually, but rather are explored in general themes.

Best practices

INHOPE outlines several best practice papers that have been or are in the process of being written. The best practice papers are among the fundamental steps used to reach goals one and two and are duly reflected in the questionnaire. This aspect of the evaluation is of particular importance considering their role in harmonizing the actions of hotlines and facilitating cooperation among key stakeholders. As these papers do not appear to be available online, an evaluation of their effectiveness is limited to responses received by those who utilize them. Accordingly, even if the best practice papers were available for review a third party cannot accurately assess their functionality. Suggestions could be made for their improvement by researchers; however, the most useful evaluation would be done in tandem with end users of the papers.

In the paper written by INHOPE entitled *The role of an Internet Hotline Network in responding to illegal use and content on the Internet* (June 2003)⁶⁵ specific mention is made of the INHOPE best practice paper on the Exchange of Reports suggesting that this particular paper is available and in use by INHOPE members. As already stated in the mapping section, all hotlines review the material reported to determine whether the content is illegal under their national legislation and then decide what appropriate action should be taken. In the cases where the content is illegal and hosted outside their country, the report is passed to the corresponding national hotline. The second hotline then takes responsibility for any additional reporting (i.e. to law enforcement or ISPs) required to deal to the material. This exchange is viewed as an effective way of combating child pornography on the Internet, as there is direct communication between the national hotlines, which removes the intermediary that is often created using law enforcement channels.⁶⁶

There is a clear logic for this system and it appears to working effectively among the hotlines within the INHOPE network. Participation in the INHOPE network creates trust among the different national hotline providers. There are minimum standards that must be met and each provider can be assured that the illegal content will be dealt with in an appropriate manner and not fall into the wrong hands. In an environment where the lives and welfare of many different people are at risk, measures must be taken to ensure that all members are trustworthy and competent. Because INHOPE has an extensive membership process, this trust is built over time within the network allowing members to demonstrate their capabilities and reliability.⁶⁷

INHOPE appears to be effective in creating stable relationships among its member hotlines. It provides, or is in the process of providing, several different best practice papers,⁶⁸ which will further harmonize and facilitate hotline activities throughout Europe. These papers will also create a common statistic format, which should assist both internal and external evaluators. Aside from personal communications regarding the functioning of hotlines and the INHOPE network, an evaluation needs objective numbers that reflect the collaboration of the hotlines both within and outside the EU. In all likelihood, these statistics are collected and need to be

⁶⁵ The paper can be downloaded from the ebsite <http://www.inhope.org>.

⁶⁶ Personal communication (November 20, 2003). Marianne Pihl, Program Manager – Save the Children, Denmark.

⁶⁷ Ibid.

⁶⁸ Best practice papers should be forthcoming regarding staff welfare, membership application forms, ART and principles of operation (Available, Reliable and Transparent) and a common statistics format.

standardized across hotlines. As stated earlier, this work is relatively new, particularly as it relates to the INHOPE network, therefore an evaluation of this detail may be premature, but it should certainly happen within the next two years.

Stakeholder relationships

Although improving relationships between many different stakeholders is not specified as a goal it is implied through the objectives. The importance of strong relationships based on the acknowledged need for collaboration or through legal agreements is evident through the writings of the EU commission and the INHOPE network.⁶⁹ In the questionnaire, there are several questions regarding the strength of relationships between hotlines and ISPs, law enforcement agencies as well as NGOs working in the field of child protection. The strength of a relationship cannot be determined by an outside party without the cooperation of those in the relationship. Therefore, the evaluation of these relationships must be done by collecting evidence from other sources.

First, national hotlines should have a strong relationship with their national law enforcement agency. The strength of this relationship will certainly vary from one country to another and may prove difficult to evaluate. The best example of the relationship between hotlines and law enforcement was provided at the INHOPE conference in Berlin. A successful law enforcement operation resulted in the capture of several pornographers. One of the hotlines was contacted to be congratulated on their cooperation but in the end, the hotline was unaware of this activity. Although this is just one example, it is probably not unique as law enforcement and hotlines must conduct themselves according to different sets of rules. These differences should be respected as each group has a very specific role to play; however, they should be minimized using a feedback system. The fact that INHOPE invited and dedicated a substantial amount of time to law enforcement during their conference speaks of their desire to strengthen these ties. The strongest relationships are built slowly and it appears that INHOPE is taking the proper steps to reinforce these bonds. Network building, however, while not the sole remit of INHOPE, must be done on local and national levels as well.

The relationships between hotlines and ISPs, as well as NGOs are quite similar. As stated in the mapping section, many hotlines have been formed by ISPs while others have been formed by child welfare organizations. It could be assumed then that the strength of the relationship with either NGOs or ISPs depends on the body that created the hotline. From the conference, it appears that INHOPE has strengthened its ties to EuroISPA as INHOPE signed an official letter of mutual understanding and presented it to the president of EuroISPA. Clearly, a relationship exists and steps are being taken to reinforce it. As NGOs have a larger area of concern, not just child pornography on the Internet, but rather the protection and safety of all children, their relationship is a bit more complex and difficult to evaluate. One of the most obvious ways that hotlines can strengthen their relationship with NGOs is by utilizing their connections and resources to reach key audiences through different venues.

⁶⁹ See Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM(2000) 890 Final; INHOPE Association of Internet Hotlines Providers in Europe, *First Report*, INHOPE, May 2002. The Report can be retrieved at the following URL: <http://www.inhope.org>.

General evaluation

The final point to discuss is the objective of INHOPE to be run in an efficient, transparent, and accountable manner. Extensive information regarding the accounting of INHOPE exists in its first report and it clearly outlines the roles of each person within the organization. From that perspective, it appears to be meeting its goal. The final facet needed to reach this goal is to have independent evaluators assess the functioning of the network. These evaluations should not be limited to hotline members but should be extended to other stakeholders. The organizations that encounter hotlines the most should be asked to assess their functioning and vice versa. Within a network, all parties should be open to critical review by all participants in order to enhance the services that are provided and strengthen existing relationships.

In sum, it appears that INHOPE is reaching its goals in an effective and timely manner. They have created a website that links directly to each member's website in addition to providing information about child pornography on the Internet, the role of INHOPE, as well as information on how individuals can help. INHOPE has created channels of communication between different hotlines and is now extending its resources to developing stronger relations between ISPs, law enforcement, and NGOs.

8.13 NATIONAL INTERNET HOTLINES

Hotlines exist in thirteen out of the fifteen European member states, of these twelve are INHOPE members. Luxembourg does not offer any hotline, in Portugal reports can be made to the Attorney General's office. Greece, although not part of the INHOPE network, offers a hotline that is co-funded by the European Union's Safer Internet Action Plan as well as by several other organizations.⁷⁰ Hotlines that are part of the INHOPE network that are outside of the EU can be found in Iceland and associate members include Australia, the United States of America and South Korea. The following review of hotlines focuses on the thirteen hotlines within the European Union.

As stated at the beginning of this section, an evaluation of national hotlines within Europe requires the cooperation of those being evaluated. The following overview of the hotlines in Europe does not portend to be an evaluation nor does it attempt to create indicators of effectiveness. As previously mentioned, in both the mapping section as well as the introduction to the evaluation, many limitations exist and these are reflected in the paucity of data available. This review of the national hotlines has been conducted through the review of secondary sources, annual reports and the assessment of the information contained within the Website of each hotline. Some of the hotlines do not offer annual reports in English, further limiting the available information. Therefore, this brief overview seeks to create a roadmap for future in-depth evaluations once the hotlines have become more firmly established.

⁷⁰ More information on this hotline can be found at <http://www.safeline.gr>.

A questionnaire for future evaluations was created, as stated in the previous section. The part of the questionnaire that focuses on national hotlines covers the following topics:

1. Standards and procedures;
2. Awareness raising and external relations;
3. Anonymity;
4. Exchange of expertise and training;
5. Care of staff;
6. General issues;
7. Non child-pornography related material.

Many of these areas cannot be evaluated using secondary sources and information must be provided by the hotlines themselves. Due to this obvious limitation, the following review attempts to highlight the positive aspects of many of the hotlines as well as those areas that may need to be addressed.⁷¹ In addition, when possible, suggestions for future evaluations are made.

Austria

The Association of Austrian Internet Providers runs *The Stopleveline* hotline, which focuses on child-pornography and Neo-Nazi related material.⁷² This hotline is notable as it has a clear logo and is easy to locate through the INHOPE website and normal search engines (e.g. Google). Their website is available in both German and English; however, the reports and information brochures are only available in German. It appears that this hotline is making significant marketing efforts by providing lapel pins, erasers, and other small things at conferences as well as offering a logo to download to be used by people interested in stopping child pornography on the Internet. Their website also provides a place where a person can ask questions and receive answers from a legal advisor. This information is not limited to child pornography but covers all types of potentially illegal content.

The Stopleveline provides statistics on their website in English while more extensive information is available in their German reports. The statistics that are available through their website suggests that they receive reports on their targeted area (child-pornography and neo-Nazi related material). Information on potential child pornography site creates the bulk of the reports. They receive an average of 14 reports per month.⁷³ This number clearly does not reflect the total number of reports as *The Stopleveline* also receives many reports regarding legal content.

Belgium

The European Centre for Missing and Sexually Exploited Children hosts the *Child Focus* hotline in Belgium.⁷⁴ This hotline is part of a larger initiative that supports investigations into the disappearance, abduction, or sexual exploitation of children. Their website is quite extensive and provides information on all of the services

⁷¹ The web address for each hotline is provided as a reference for each of the National Hotlines. All the information provided in the following summaries was taken either from the annual report (available on the website) or from the first INHOPE report.

⁷² <http://www.stopleveline.at>.

⁷³ Does not include data for November or December 2003.

⁷⁴ <http://www.childfocus-net-alert.be>.

available. The Belgian hotline allows for anonymous reporting and allows users to report in a variety of formats. Like Austria, there is a question and answer section devoted to many different topics.

The annual report for *Child Focus*⁷⁵ provides statistics on the number of reports received and what actions were taken with the reports. During 2002, Child Focus received 2274 reports of potential child pornography, which is an approximate average of 190 per month. These statistics are further broken down into the type of media that is used. This type of detailed reporting is useful for evaluators and program administrators as one is able to determine the level of utilization by the public and appropriately focus resources on the medium that contains the highest percentage of child pornography. In Belgium 57.9% of the reports focused on websites confirming the fact that the focus should remain on that area.

The other statistic, which would be useful to evaluators, is the typology of the reported sites. This information addresses the issue of whether or not the reports that are sent are representative of what is being sought, in this case, child pornography. According to their statistics, of the reports that were sent on to federal police a third of the sites were child pornography while 4.1 % were a mix between both child and adult pornography.

The statistic, however, that provides the most insight to evaluators is that 42.5% could not be qualified by *Child Focus* due to lack of feedback from the Federal Police. This provides evidence of potentially limited cooperation between the hotline and law enforcement agencies. Law enforcement needs to be encouraged to provide information to hotlines in order to ensure that they are effectively targeting their message to receive the desired types of reports.

Denmark

The Danish hotline, known as *Red Barnet – Save the Children*,⁷⁶ is a nation-wide non-governmental organization that focuses on the prevention of child sexual abuse. This hotline is only focused on the protection of children and does not concern itself with other illegal content. *Red Barnet* provides an annual review that outlines the importance of the fight against the sexual exploitation of children as well as the hotline's activities. In 2002, the Red Barnett hotline received 6483 reports or an average of 540 reports per month. Of these reports, 46% contained either child pornography or child erotica. It appears that the strict focus of Save the Children increases the number of reports received from the public.

Red Barnett demonstrates their utilization of the network created by INHOPE as 58% of their reports were passed on to other hotlines. Within the annual report, they also state that 23% of their reports are forwarded to law enforcement. Their annual report provides information suggesting that this hotline has strong relationships with many stakeholder groups and could provide useful advice to other hotlines.

There are several remarkable characteristics of the Danish hotline. One of the most notable aspects is the fact that they pass on reports to VISA in order to limit access to pay sites. Thus, they have been able to create viable relationships in both the public and private sector, all the while maintaining a single focus. Furthermore, although the staff does not appear to be that large, the employees come from a psychological or social service background. This enables them to provide the

⁷⁵ Annual report 2002 childfocus-net-alert. Available to download from <http://www.childfocus-net-alert.be>.

⁷⁶ <http://www.redbarnet.dk>

necessary human touches that are sometimes lacking when the attention is placed too heavily on technology. By focusing strictly on child protection issues, it appears that they are able to dedicate their resources to provide the best service possible. Finally, and perhaps, most importantly the staff of this hotline publishes information on child exploitation and provides lectures to children and caregivers in an effort to increase the safety of children.

Finland

Save the Children, Finland runs the hotline *Pelastakaa Lapset – Rädda Barnen*.⁷⁷ Similar to Denmark, their sole focus is on the protection of children. The website is available in both Finnish and English. Unfortunately, there is no clear reporting place for child pornography or obvious information regarding the hotline services that are provided. The annual report for Save the Children-Finland covers all of their activities and mentions that it recently started work on protecting children from dangers inherent to the Internet.

France

The hotline that is available in France is entitled *Point de Contact*⁷⁸ and was established by an Internet Service Provider association. A review of this hotline is limited by the fact that the website is presented largely in French with minimal English translation. There is a clear place to report illegal content with corresponding directions about the type of information required to make a report. The section containing the directions on how to make a report is provided in both French and English. In addition, there is a section dedicated to safety on the Internet. Some of the pages are designed with children in mind, while the other pages have fewer cartoons and appear to be geared towards adults. *Point de Contact* does not seem to have an annual report, thus limiting any further secondary source evaluation.

Germany

In Germany, there are three initiatives, all of which are INHOPE members and each of which focus on different areas. The first is the *eco Forum*,⁷⁹ this hotline is part of an industry association specializing in newsgroups. This forum takes a proactive role by monitoring the contents of newsgroups and has recently launched a hotline. The information is only available in German therefore a comprehensive review is not possible. The other two bodies in Germany are *FSM* and *jugendschutz.net*.⁸⁰ Both of these bodies focus on complaints regarding the World Wide Web. *FSM* is a private self-regulation body; their website is available in German, English, French, and Spanish allowing users from a large part of Europe to utilize their website. The complaint form is also available in all four languages and is relatively simple to complete. As Europe is such a multilingual society, the example set by *FSM* should be followed by as many hotlines as possible. The publicly funded body *jugendschutz* provides information only in German. A large amount of information is available on their website, including downloads for rating and filtering content.

⁷⁷ <http://www.pela.fi>

⁷⁸ <http://www.pointdecontact.net>

⁷⁹ <http://www.eco.de>

⁸⁰ <http://www.fsm.de> and <http://www.jugendschutz.net>

Greece

Many different partners including Safenet, a self-regulatory body, ITE, a research body as well as several other Greek institutions created *The Safeline*.⁸¹ As stated previously *Safeline* is not part of the INHOPE network but is nonetheless co-funded under the Safer Internet Action plan. *The Safeline* website has several notable features as it is presented in both Greek and English with an obvious place to send reports. Clear information is provided about sending reports, how the information will be used as well as a discussion regarding anonymity. The Greek website is simple and easy to use, with information that relates only to the topics that concerns that hotline (e.g. child abuse, racist and xenophobic material or other illegal material). The website does not provide any type of statistical data nor does it provide an annual report.

From an evaluation perspective, it would be interesting to compare the number of reports sent to and received by Greece to other countries that are part of the INHOPE network, in order to measure the effectiveness of those things that Greece does not have in common. In addition, it would be important to evaluate the follow-up of reports originating from and sent to Greece considering they are not part of the INHOPE network. The example of Greece highlights the importance of evaluating all hotlines, not just the members of the INHOPE network from the perspective of all the important stakeholders.

Ireland

*The Hotline*⁸² is funded by the Irish Internet Service Providers Association and has very close ties to this group. From a review of their website, it appears that there are many different ways to report child pornography and substantial information exists for all age groups. Furthermore, there is an annual report reflecting the work done from November 1999 to June 2001. Although, the data available is not up-to-date it provides an insight into the functioning of the hotline and some of the difficulties that are encountered.

This report provides statistics on the way in which reports are received. In the vast majority of cases, users prefer to use the hotline website. This hotline also appears to be successful in that the types of material reported are mostly child pornography related, suggesting that they are not spending substantial time focusing on other issues or reports. Although extensive statistics are not provided, insights into the difficulties that face the hotline are. For instance, many of the reports are incomplete or difficult to track down requiring a significant number of man-hours. In addition to the annual report, there are a number of press releases reflecting the activity of the hotline as well as the various stakeholders. The difficulties outlined in both the report and the press releases should be more completely evaluated in order to provide a solution for all hotlines, which surely face similar problems.

The number of reports received by *The Hotline* seems to be lower compared to some other hotlines. This point is difficult to evaluate without a standardized measuring tool but perhaps more extensive awareness campaigns are needed for this particular hotline. As *The Hotline* is an integral part of the Irish Internet Service Providers Association, it is possible that more networking is required with other stakeholders less involved in the industry (e.g. NGOs, law enforcement etc.). Their annual report provides an excellent template for other hotlines, as there is a mix between qualitative and quantitative information enabling evaluators and other

⁸¹ <http://www.safeline.gr/index-en.html>

⁸² <http://www.hotline.ie>

interested persons to understand what are the strengths as well as what are the areas of concern for that particular hotline.

Italy

*Stop-it*⁸³ was launched by Save the Children, Italy and is part of the INHOPE network. In addition, *Stop-it* collaborates with the Italian ISP, Ecpat Italy and several consumer groups. There is an annual report that was not yet available for download at the time of writing. As it works under the Save the Children umbrella organization, its focus is similar to that of Denmark. However, different from other Save the Children sites, the first webpage one visits is that of the hotline as opposed to the Save the Children website. The *Stop-it* website is similar to other hotline sites as there is a section on frequently asked questions and a place dedicated to general resources that could be of interest to users. This website, itself, is only available in Italian; however, the reporting form is provided in both Italian and English.

Spain

OPTENET, a filtering company, launched the *Protegeles*⁸⁴ hotline, which is also run in conjunction with Acción Contra la Pornografía Infantil (ACPI) the Spanish representative at the European Federation for Missing and Sexually Exploited Children. The *Protegeles* website accepts reports related to child pornography, terrorism, racism, and drugs. There is an obvious reporting area when visiting the website, unfortunately there is no information regarding personal information. In fact, it appears that they do not collect any personal information about the reporter at all. This may discourage some reporters who would like to have follow-up contact with the hotline to ensure their report was received.

The Spanish hotline has been a front runner in the area of legal issues related to hotlines with the publication the Legal Manual for a Spanish Hotline battling against child pornography on the Internet.⁸⁵ This study, carried out by K.U. Leuven Research and Development, could serve as a model for other hotlines throughout Europe to address issues related to privacy, employee contracts, public authorities, ISPs and other interested stakeholders. In addition to this important study, the *Protegeles* website offers a number of press releases, which provides an insight into their collaboration with other stakeholders. Obviously self-selected press releases are naturally biased; however, they do provide an additional source of information.

Sweden

*Rädda Barnen*⁸⁶, the Swedish Save the Children Organization hosts their hotline and has many of the same goals and activities outlined for Denmark. Again, this hotline benefits from the single focus of child safety and builds relationships with the public utilizing that message. The employees of *Rädda Barnen* also provide lectures and do public outreach with a variety of stakeholders. The website is available in both Swedish and English; unfortunately, it is very difficult to find the reporting area or an area that is specifically dedicated to reporting child pornography found on the Internet.

⁸³ <http://www.stop-it.org>

⁸⁴ <http://www.protegeles.com>

⁸⁵ *Protegeles*, Spain, *Legal Manual for a Spanish Hotline battling against child pornography on the Internet*, available online at <http://www.protegeles.com/informes/LEGALMANUAL.pdf>

⁸⁶ <http://www.rb.se>.

The Netherlands

As stated on the INHOPE website 'Meldpunt'⁸⁷ is a private body established by concerned Internet users, the Internet industry, and law enforcement' The larger organization provides an English website explaining that the Meldpunt organization focuses of complaints of a discriminatory nature; however, part of this organization Meldpunt Kinderporno focuses on the removal of child pornography from the Internet. The website dedicated to child pornography is provided only in Dutch and does not have a very clear place to report illegal material. Their website, however, appears to offer ample amounts of information.

United Kingdom

*The Internet Watch Foundation*⁸⁸ is a private body funded by the Industry. This hotline sets an excellent example for transparency and annual reports, which date back to 1997. The 2002 annual review outlined all the actions, the supporting reasons and the hoped for outcomes taken by the hotline. This report also provides an outstanding section devoted entirely to statistics such as the number of reports received, how much they have increased over time and how many arrests have been directly related to the information provided by the hotline.

One noteworthy statistic, which may speak of the organizational integrity of IWF, is the fact that they receive over 400 complaints per week! This is an astonishing number and highlights the effectiveness of their campaigns to gain visibility among the public. The IWF has very few employees and a substantial funding structure that clearly seems to work efficiently and produce the desired results. In fact, over a six-year period IWF has seen the number of reports steadily rise to the year-end total in 2002 of 17868. An evaluation of this hotline would prove beneficial to the entire network as one could identify what is working for them and why and implement the necessary changes in the remaining hotlines.

⁸⁷ <http://www.meldpunt.org>.

⁸⁸ <http://www.iwf.org.uk>.

8.14 CONCLUSIONS

To conduct an evaluation of all the hotlines in Europe is fraught with difficulties. The INHOPE network will certainly ease the way as the hotlines become more standardized and the statistics gathered are of a comparable nature. The mapping conducted in the first part of this report provides a good starting point for an evaluation. The second task sought to build upon that mapping and provide an evaluation of the effectiveness of prevention measures instituted in EU Member States. As there were significant difficulties in carrying out a full-scale evaluation of hotlines a tool was created that could be used for all types of hotlines regardless of their INHOPE membership. Each country was then reviewed to determine if they provided the basic requirements for a secondary source evaluation. In many cases there were annual reports, however not all were available or were written in the original language. The latter will obviously require substantial linguistic resources and could prove to be a limitation. Each website was visited to gather as many secondary sources as possible; once those were reviewed, it became clear that a complete evaluation required insider knowledge not readily available to the public. An effective hotline does not simply consist of a good website and a place to report potentially illegal content, human resources need to be measured and assessed, comparable statistics must be gathered and a sufficient sample of stakeholders should be queried. Once these steps are completed, one can provide a thorough evaluative summary and make suggested changes for all stakeholders.

From the review, it is clear that many of the hotlines have notable features that may be of use to other hotlines throughout Europe. For instance, Ireland and the UK offer excellent annual reports, which provide important insights into their functioning. Hotlines that are part of the Save the Children organization benefit from a single focus of protecting children; yet, the hotline may suffer because the websites do not always provide a very clear place to report suspected child pornography. The diversity and creativity demonstrated in each website should be encouraged; however, standards relating to ease of reporting must be respected if the network is to function properly. In line with similar standards, common and comparable statistics should be created in order to measure the efficacy of hotlines throughout the INHOPE network.

To conclude, the working seminar brought practitioners in contact with these findings and provided additional insight into the functioning of hotlines as well as what role they can and should play within this area. It was noted that there must be a distinction between preventing child pornography on the Internet and keeping children safe while they are surfing the web. Although these are fundamentally different, each feeds into the other in that if children are safer while surfing the Internet they are less likely to fall victim to perpetrators. Preventing child pornography on the Internet is a large topic that includes preventing its circulation as well as trying to keep children safe. Hotlines have expertise to offer in both areas vis-à-vis their ability to reach diverse audiences and inform them of safety issues as well as through accepting reports to reduce the amount of child pornography available within the web-based environment. In line with this topic, child pornography is not always pictures of abuse and can be of young people exploring their sexuality, which is then released onto the Internet. Hotlines, in this instance can provide advice to these young people about what to do about these pictures and how to avoid that situation in the future. Thus, hotlines have a diverse role to play in keeping children safe on the Internet and can assist victims by providing

information on where they can go for help. Furthermore, this victim assistance can also be extended to law enforcement agencies that come in contact with victims.

An important question posed by hotlines is, are they reaching their target audiences when trying to increase the visibility of the issues and the hotlines? One of those audiences may be consumers of adult pornography who may be more likely to come across child pornography while surfing the Internet. The Belgium hotline identified this possibility and set up a booth at erotic shows in several Belgian cities in order to reach this target group. However, hotlines have a delicate balancing act to play; they cannot encourage people to proactively search for child pornography, yet they ask for reports to be sent in when these images are found. One of the advantages provided by INHOPE is that all hotlines within the network are able to come together over the course of the year and discuss what is working and what needs to be changed.

One point brought up repeatedly during the seminar is the importance of increased collaboration and having a single point of contact within each country. In essence, it is impossible to expect someone from Germany to be an expert on the laws, idiosyncrasies and proper people to contact in Spain. Thus, working seminars and single points of contact are virtually indispensable. The single point of contact should know who to speak to and be familiar with their system making the 'outsider' an 'insider' by virtue of their knowledge. Additionally, a single point of contact simplifies the system, reduces repetition of work and allocates resources more effectively. Hotlines are in the unique position in that they can provide this single point of contact for users, industry and law enforcement. It appears that one well-funded hotline is sufficient or there is the risk of confusion. This point, however, should be researched further in order to determine the most effective way of providing hotline services to users that cover a wide range of topics while still striving to create a single point of contact.

Related to the single points of contact, it is important to identify the most appropriate stakeholder to carry out the necessary tasks within this campaign against child pornography. It emerged that INHOPE and the national hotlines are not allowed to launch awareness campaigns due to the strict EU regulations regarding spending. This seems to be a mismanagement of valuable expertise as hotlines are unable to draw upon their resources and existing connections to perform awareness raising activities. Instead, they must outsource this task to another group who may or may not be as knowledgeable in the area as hotlines.

Working for a hotline, or in any other capacity, related to child pornography is traumatic and difficult work. The human aspect of the people working in this field must not be overlooked and the practitioners must be properly cared for psychologically. INHOPE has created a best practice papers regarding care of staff; however, many hotlines still suffer from high turnover suggesting that more attention needs to be paid to the area. Some of the suggestions provided were forced time off over the course of a several years, ongoing psychological counselling during the individuals employment as well as having several duties to perform such as teaching children in schools and writing papers in addition to the task of reviewing illegal material.

It was also concluded that there must be a system of sustainability for the stakeholders. This is something that must be implemented on both the national and international level. Funding rules should be flexible enough to allow many different parties to contribute. Relying on one source of funding, be it, the European Commission or national sources is a risky proposition should that source

choose to reallocated funding. A prime example is the website www.saferinternet.org, which was an excellent 'one-stop shop' for information on Internet initiatives developed throughout the European Union; unfortunately, this website will no longer be updated because they were not granted additional EU funding.⁸⁹

Finally, and perhaps most importantly, the Internet is a global phenomenon and many reports come from countries with less developed legal codes and regulations. Most of the countries that will soon be joining the European Union are now presented with the opportunity to put effective systems in place to combat child pornography; however, they remain reticent, as they believe that since they have low levels of Internet penetration that these systems are unnecessary. These countries are in a prime position to be proactive rather than reactive and this should be encouraged at all levels. One possible way of doing this is create an EU funding structure that works together with national funding bodies to help build the necessary infrastructure in the targeted country. For example, Germany can pair with Hungary using the resources and knowledge from all three groups to create an effective and efficient system within that particular country.

⁸⁹ Seminar Communication (January 16, 2004). Thomas Rickert – INHOPE President, Brussels Belgium.

9.

FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION C (AWARENESS AND EDUCATIONAL INITIATIVES) BY WORD & PICTURE LANGPORT AND UNICEF – INNOCENTI CENTRE FIRENZE

9.1 EVALUATING PREVENTIVE MEASURES IN ORDER TO IMPROVE THEIR EFFECTIVENESS IN THE EU MEMBER STATES, BY WORDS & PICTURES, LANGPORT⁹⁰

This Commentary and Additional Information was prepared by the Words & Pictures consultancy, based in Langport, United Kingdom, in the framework of the project on “Child pornography on the Internet: Evaluating preventive measures in order to improve their effectiveness in the EU Member States”, awarded in December 2001 (contract 01/097/C signed on 12 December 2001) by the Daphne Programme – European Union, and managed by Transcrime – University of Trento.

This Commentary and Additional Information should be read in concert with the Report prepared by the UNICEF Innocenti Research Centre (IRC), based in Florence, Italy, on social and educational initiatives in relation to child pornography.

This Commentary and Additional Information aims to enhance the information available in the IRC Report with the input and reflections of a multi-sector group of experts gathered by Transcrime for a seminar in Brussels in January 2004, as well as other online and offline sources with experience and expertise.

Thus it reviews the key issues set out in the IRC Report, especially the lack of a comprehensive and coordinated network working on social and educational initiatives, limitations of past and present awareness campaigns, the need for national “nodes” for liaison, and questions about the effectiveness of initiatives.

It also highlights points raised on social and educational initiatives at the seminar, especially the need for integration of efforts to encourage safer surfing, opportunities for pan-European campaigns and the role of the EU, issues of sustainable funding and doubts about the connection between child pornography and child protection

This Commentary then explores the present disconnect between protecting children and preventing child pornography, offers recommendations based on the IRC Report and seminar discussions – from coordination to the role of mass media and new risks in communications technology – and lists useful sources on social and educational initiatives in relation to “Child pornography on the Internet: Evaluating preventive measures in order to improve their effectiveness in the EU Member States”.

Words & Pictures is grateful to all the experts from law enforcement agencies, ISPs, hotlines, child protection groups and other institutions who participated in the Transcrime seminar in Brussels in January 2004, as well as those experts who contributed to the UNICEF–IRC Report.

Thanks are also due to June Kane for her unique contribution to this work.

⁹⁰ Words & Pictures, Tudor Saint Anthony, Muchelney, Langport, Somerset TA10 0DL, United Kingdom, +44 1458 251727, wordspicturesuk@yahoo.co.uk.

Finally, Words & Pictures is grateful for the support of the Transcrime secretariat.

9.1.1 Key Issues Arising from the UNICEF-IRC Report

Any report on the internet and the social and educational initiatives responding to concerns about its risks for young people can only be a snapshot of what is happening and is thus immediately out of date in terms of this fastest moving of all media.

Despite this caveat, the IRC Report offers a clear EU-wide picture, in which almost every country has social and educational initiatives, reflecting wide awareness of online safety and child pornography issues, and the EU Community Action Plan has supported many initiatives, with nearly all initiatives involving NGOs.

While acknowledging gaps in reporting by governments and other actors, which may underestimate levels of social and educational initiatives, the IRC Report finds that:

- only 13 countries involved education authorities in “safer surfing” initiatives;
- only 10 countries had national or regional initiatives aimed at children;
- only 9 countries had activities involving internet service providers (ISPs);
- only 8 countries had public awareness campaigns for safer internet use.

Social and educational initiatives that aim to be part of measures to prevent internet child pornography are very diverse, use different materials, involve a varying range of institutions and reflect national differences in attitudes, internet access and other factors. They form a “patchwork” of activities, rather than a fully connected network.

Despite the number of multi-country initiatives, including Safer Internet For Knowing and Living (SIFKaL), Dot.Safe, Educaunet and Safe Borders, many of the campaigns so far have been short term, partial or pilot schemes.

The various actors involved do not necessarily work closely together; for example, experts consulted by IRC did not know how far law enforcement agencies were involved in social and educational initiatives. The media have not often been directly involved in such initiatives yet carry alarming news reports on child pornography or paedophiles that suggest a lack of understanding of others’ work. Government-led initiatives appear not to offer much support for collaborative work by NGOs.

There are worries about whether EU funding for social and educational initiatives will decline as child pornography is only one issue among a growing range of internet problems – such as hate crimes or gambling – competing for attention and resources.

Different approaches – government-led education initiatives, industry self-regulation and hotlines, child welfare from NGOs – may not be complementary and without sufficient assessment to offer an optimised multi-sector approach, according to the IRC Report, while it found limited coordination of the existing initiatives within countries or between them, with few national “nodes” for liaison, information sharing, collation of expertise or evaluation of strategies.

While the sustainability of social and educational initiatives is crucial to reach the flood of new internet users and reinforce caution among existing users, few countries – so far the UK, Italy, France, Germany, Netherlands – have established permanent structures for this work, and some of these are charities lacking permanent funding, rather than government bodies.

There is a need for simple messages and concepts when the problem is complex and fast-changing, and to adapt materials well to diverse audiences. This is especially important to avoid campaigns highlighting Internet dangers that can attract risk-taking behaviour and unfortunately promote what they aim to prevent.

Key advice on the components of social and educational initiatives includes:

- Avoid alarmist language or merely warning about dangers.
- Help children develop an autonomous, responsible attitude to the internet.
- Complement other protection methods: filters, security controls, classification.

Key advice on the objectives of social and educational initiatives includes:

- protect children from harmful content or risks from other internet users;
- direct children to positive material and experiences available on the internet;
- develop net literacy so children protect themselves and use the internet well.

While self-regulation and end user autonomy are central to present approaches, this does not imply that there should be a hands-off approach by governments or ISPs.

The IRC Report assumes that “effectiveness” can be measured in terms of reaching young Internet users, based on the multiplicity of actors and means used, coverage and outreach, and sustainability. Yet this method appears to offer limited quantifiable evidence of children reached, behaviour changed or child pornography prevented.

While many different actors are involved in campaigns, there are few cross-sectoral campaigns involving several simultaneously to reinforce messages, which may reflect the lack of national nodes to coordinate activities and share the work and costs.

Channels used for social and educational initiatives vary from country to country, with the internet used in all cases, printed materials used in most, fewer using radio or press and only seven countries using the best medium to reach children: television.

The variety of social and educational initiatives has produced a wide range of materials, messages and strategies. Many are being tested, adapted and translated, offering a good basis for future action, especially in schools and on the web. But the European Commission has expressed concern about the cost effectiveness of some social and educational initiatives, since their impact on small audiences may need major expenditure when scaling up to national or pan-European levels.

While the need for social and educational initiatives to help encourage safer surfing is obvious, the response across Europe appears to have been patchy and – by the internet’s standards – slow, with limited coordination or sustainability.

9.1.2 Key Issues Arising from the Seminar of Experts

Social and educational initiatives were among subjects discussed at a Transcrime seminar involving a full range of experts and institutions dealing with Internet child pornography and preventive measures from many EU countries.

Participants' comments focused on four main areas of concern: integration and multiple stakeholders, the EU's role, sustainability and funding, and clarifying the connection between child pornography and child protection.

Individuals from various sectors affirmed the need for joint action to increase the opportunities for successful communication, share knowledge of best (and worst) practice, and spread costs, rather than relying on single-sector initiatives or small coalitions.

In a similar way, there was support for messages to be delivered through many channels and networks, from various forms of mass media to membership organisations, since this would again maximise impact.

Among the comments:

- "Politicians decided that prevention was not a police issue. Prevention should be the combined focus of many organisations", and: "Technology alone is not the answer – it needs a holistic approach."
- "Children need activities more than advertising, and we need multi-organisation partnerships", and: "You need a multiplier effect, working through various networks and associations of parents and teachers to reach the biggest audiences."
- "We need to be using all media, from TV to new mobile technologies. We need to educate parents about mobile technologies and teach teachers about Internet relay chat", and: "We need cross-sectoral campaigns. The key is to have partners so messages come from different directions."
- "There have been a lot of different initiatives. Are all of them needed? Are any a waste of money and resources?" and: "Everyone is brewing their own soup; they're not talking to each other."

The patchwork of social and educational initiatives brought suggestions for European action to collate and share good practice and materials, and for the creation of pan-European social and educational initiatives.

Among the comments:

- "We've never seen something on a European-wide basis", and: "Why not have one Europe-wide campaign to show people this is a European concern and there is European commitment."
- "Pool information so everyone can see other campaigns and, with EU help, collate the URLs to lead to all available materials", and: "It is important to have European coordination with local adaptation of campaigns and ideas."

Perhaps inevitably, the limits of existing resources was one topic, with participants concerned that other internet content – from gambling sites to xenophobic material – would draw attention and funding away from protection of children and prevention of child pornography, or that there might be competition for limited funds rather than collaboration between the sectors concerned with the internet.

The point was also made that more is required than one-off social and educational initiatives since internet use is expanding, new generations of children are reaching an age when they will use the internet, and the range of hazards is growing. Thus the need for sustained, effective, evolving campaigns that have demonstrable results.

A number of experts highlighted the need to keep a distinction between safe surfing advice and the issues of child pornography (see next section) since children were far more likely to come across other forms of harmful content during unsafe surfing.

While the IRC Report does not mention any efforts to reach the two groups most likely to come across child pornography – the producers and users of other forms of pornography – this issue was raised at the seminar.

Participants were told about two efforts – one in Belgium and one in the United States – made to take awareness campaigns about child pornography to the providers of other pornography, both by taking exhibition stands within adult content industry trade shows.

These efforts were aimed at encouraging both the producers and users of adult content to report child pornography, and offering producers ways in which they could help this process by adding reporting links to their web sites.

Information was shared about one country's use of "honeytrap" false web sites in which law enforcement officers set up dummy sites that warned visitors – after they had persisted in trying to access material through several stages – that they can be tracked and arrested if they view such material.

Educational initiatives cited included interactive computer games with clues that children had to solve, or classroom-based computer chat sessions that finally revealed that the "girl" the school students had been messaging was really a policeman. Both offered strong impact but at a high cost because of the staffing involved.

While the seminar shared information about many positive actions in technology and law enforcement to prevent child pornography on the internet, as well as discussing initiatives to protect child internet users, there was some pessimism.

This ranged from the simple observation: "It is very difficult to prevent children from accessing harmful content", to the comment: "The social environment is not progressing as fast as the Internet. It may take until today's children become parents and can teach their own children."

[NB: "Comments" are summaries rather than exact quotes.]

9.1.3 Child Internet Safety and Child Pornography

Social and educational initiatives aimed at children and their parents and teachers have done little to prevent child pornography on the Internet, to judge by the IRC Report and comments at the Transcrime seminar.

While it is obviously important to protect children from harmful material and paedophiles, the links between these two dangers and child pornography is not clear, and it is unhelpful to ignore or confuse these issues' complexities, since that could waste the limited resources available and result in less being achieved.

Most harmful Internet material – by any definition – is not child pornography, but other pornography, gambling, hate crime sites, and further sorts of anti-social content. Much of this is on password-protected sites, or requires credit card payment, or could be barred from access by safe surf software, classification or ISP screening.

Law enforcement agencies suggest that producers and users of child pornography are today largely avoiding the open internet's legal risks in favour of password protected sites, public peer-to-peer file sharing, "dark networks" of private peer-to-peer systems and other mechanisms, all of which are less easily accessed by children.

While most paedophiles collect child pornography and some use it in the "grooming" of potential victims, the risk from paedophiles contacting children over the internet – in chat rooms and elsewhere – is far more immediate in terms of their personal safety if contact leads to a meeting rather than the production of child pornography.

Some child pornography no doubt results from abduction following paedophile cyber stalking, and organised crime is involved in pay sites originating in Eastern Europe. Yet it appears that the majority of people producing such material – like the majority of child abuse perpetrators – are family members or "friends", neighbours or adults who have access to a child through positions of authority, youth organisations etc.

However, links between child Internet use and child pornography on the Internet are getting closer. Since child abuse victims are more likely to abuse children themselves, and paedophile tendencies can begin at around the age of 12, the internet's risks may be far more potent for certain children. How can social and educational initiatives help these vulnerable – and potentially dangerous – children?

There is also the growing use of digital cameras, web cams and camera phones that can be used by children – with or without adult prompting – to produce images that can end up on the internet of themselves, family members or friends.

The phones hold other dangers: despite promises to protect children, mobile telecom operators are planning to offer services with "adult content", while in Japan, where child mobile phone ownership is very high, child prostitution is often initiated by adults approaching children through their mobile phones.

9.1.4 Some Recommendations

Based on the IRC Report, the Transcrime seminar and other sources, some recommendations and suggestions for future social and educational initiatives, including awareness campaigns and promotion of safer surfing:

1. Governments and the EU should ensure they assist the coordination, integration and sustainability of social and educational initiatives over safer surfing and harmful content, including the hotlines that should be a part of every awareness campaign
2. Governments and the EU should support multi-sector and multi-channel campaigns over single-sector or single-channel efforts, so social and educational initiatives are well integrated, cost effective and have a better chance of reaching their targets.

3. This should involve the creation of and support for national “nodes” for cooperation and liaison within each state and between states. While these do not have to be government-owned or -led institutions, they require sustainable funding.
4. There should be further support to develop strategies, materials and systems of monitoring and evaluation for social and educational initiatives, as well as the means to share these tools and techniques through events and training, web sites and DVDs.
5. Lessons should be drawn from successful commercial and non-commercial communication campaigns and tactics that alter child behaviour, attitudes or spending, from those about drugs and alcohol, sexually transmitted diseases and pregnancy, clothing and soft drinks to music downloads, viral marketing and urban myths.
6. Involve mass media since they can play a crucial role in ensuring that the public understanding of child internet issues is one of informed concern not moral panic, as well as offering information that assists decision makers in their judgements.
7. Help children further develop safe tools and tactics so they can inform, educate and protect each other, rather than rely on adult-led campaigns that they will automatically discount.
8. Support is required for awareness campaigns that aim to reach the two groups most likely to come across child pornography: the producers and users of other adult content.
9. Given that most child pornography – in terms of content on internet servers – is located outside the EU, improve learning from and communication with institutions dealing with child pornography in the United States, Asia and other parts of Europe.
10. Consider now the risks of new technology – especially the capacities of mobile phones – so future social and educational initiatives can be pro-active and pre-emptive rather than too little, too late.

9.1.5 Sources and Further Information

EU Internet Action Plan

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

EU Safer Internet

<http://www.saferinternet.org/>

Consumer Internet Safety Awareness

<http://www.net-consumers.org/erica/indexs.htm>

Dot.Safe

<http://dotsafe.eun.org/>

EDUCAUNET

<http://www.educaunet.org/>

INFONET

<http://www.capitannet.com>

INHOPE (Internet Hotline Providers in Europe)

<http://www.inhope.org/>

Net Protect

<http://www.net-protect.org>

ONCE (Online Networked Children's Education)

<http://www.once.uclan.ac.uk/>

Safe Borders

<http://www.safer-internet.net/>

SAFT (Safety, Awareness, Facts and Tools)

<http://www.saftonline.org/>

SIFKaL (Safer Internet For Knowing and Living)

<http://www.sifkal.org>

SUI (Safer Use of Internet)

<http://www.helpnet.at/>

SUSI (Safer use of Services on the Internet)

<http://www.besafeonline.org/>

9.2 EVALUATING PREVENTIVE MEASURES IN ORDER TO IMPROVE THEIR EFFECTIVENESS IN THE EU MEMBER STATES, BY UNICEF INNOCENTI CENTRE, FIRENZE

This Report was prepared by the UNICEF Innocenti Research Centre (IRC), based in Florence, Italy, in the framework of the research project on 'Child pornography on the Internet: Evaluating Preventive measures in order to improve their effectiveness in the EU Member States', awarded in December 2001 (contract 01/097/C signed on 12 December 2001) by the Daphne Programme – European Union, and managed by Transcrime – University of Trento.

This two-year project seeks to assess the effectiveness of the preventive measures enacted, throughout the EU, in the field of child pornography on the Internet, and to contribute to their improvement. This is to be achieved by collecting information and developing a framework model to evaluate the effectiveness of such measures. The findings of the analysis are then to be turned into concrete tools for the operators in the field. The main expected results of the project are a report outlining the findings of the effectiveness evaluation and a practical *vademecum* addressed to the operators.

For its part, the UNICEF-IRC Report maps out awareness and educational initiatives in force in the EU Member States against child pornography on the Internet and proposes a framework model to evaluate the effectiveness of such measures. These aspects of the overall project correspond to activities foreseen during its first year.

UNICEF–IRC carried out the mapping and preliminary evaluation between February 2002 and June 2003. The Report constitutes a synthesis of information gathered from responses to a specially developed questionnaire as well as from websites and wide-ranging documentary research conducted in the legal and practical fields.

9.2.1 Section A: Background

It is worth recalling, as we begin to examine the development of awareness and education initiatives regarding child pornography on the Internet, just how recent the phenomenon is – and thus how short a time has been available for devising, implementing and evaluating such initiatives. Recognition of the potential problems that the Internet could generate for child protection began to produce expressions of serious concern only as of the mid-Nineties. In her speech at the opening session of the 1996 1st World Congress on the Commercial Sexual Exploitation of Children, European Commissioner Anita Gradin noted that:

'[c]hild pornography and networks between paedophiles are but some of numerous problems we will encounter as we enter the information society. The European Commission is already looking into this problem. It will in the near future propose action to various kinds of offending use of information networks, such as Internet... As governments and parliaments pursue their work to adjust legislation to new media techniques, such as video, television and computerised networks, they must safeguard the freedom of expression. But it is equally important that our children are protected against abuse of modern technology.'

But these were early days, and the Declaration and Agenda for Action emanating from that same meeting contained no explicit reference to child pornography on the Internet: the closest it came was to mention the need for 'the computer and technology industry', amongst many others, 'to monitor and report cases [of sexual exploitation] to the authorities, and to adopt voluntary ethical codes of conduct.'⁹¹

The explicit attention paid by the European Union to the prevention of child pornography, and particularly of child pornography on the Internet, indeed dates back to 1996, as Ms Gradin noted. And as of that time, other international organisations with a wider constituency – including the United Nations⁹², UNESCO and the Council of Europe – also began taking initiatives focusing on, or encompassing, issues relevant to this sphere.

Thus, in 1997, the UNESCO International Clearinghouse on children, youth and the media, co-financed by UNESCO and the Government of Sweden, was set up to promote awareness and knowledge in this field. The Clearinghouse, located at Nordicom⁹³, seeks to contribute to policy-making, public debate and children's media literacy and competence. Among its relevant products is a worldwide register of organisations concerned with children and the media.

⁹¹ Even the Global Commitment from the follow-up Congress (Yokohama, 2001) makes only a laconic explicit mention, with the commitment to 'take adequate measures to address negative aspects of new technologies, in particular child pornography on the Internet (...)'.

⁹² UN Convention on the Rights of the Child ; UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child prostitution and Child pornography

⁹³ Nordic Information Centre for Media and Communication Research.

The January 1999 expert meeting at UNESCO headquarters on 'Sexual abuse of children, child pornography and paedophilia on the Internet' sought to assess what had been achieved to date by UN specialised agencies, governmental and non-governmental organisations, the Internet industry, law enforcement agencies and the media regarding

the safer use of Internet, with a view to orienting future efforts. The 2-day meeting approved a Declaration and an Action Plan.⁹⁴

Among its most recent initiatives, the Council of Europe published in 2002 the replies to a questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services.⁹⁵ Information was collected on initiatives undertaken in nineteen of the Council's forty-four Member States, plus Canada, in the field of regulation of illegal and harmful cyber content, and it is updated on a regular basis. The data reveal differences from one country to another, but also some common approaches and types of initiatives, whether public or private, concerning the means to regulate the Internet. Through its website, the Council of Europe aims to gather a maximum number of contributions from a wide range of sources so as to develop a vast information platform for raising awareness on safer Internet issues.

For its part, the UN Committee on the Rights of the Child regularly expresses its interest in whether or not campaigns have been carried out to raise awareness of the danger to children of the availability of harmful material on the Internet, and whether any in-depth study has been carried out to improve understanding of child pornography. It also asks about the procedure to follow if children wish to report problems. The Committee has regularly encouraged continued consideration of the recommendations set out in the Agenda for Action adopted at the World Congress against Commercial Sexual Exploitation of Children held in Stockholm in 1996.⁹⁶

⁹⁴ For details, see UNESCO's web site: http://www.unesco.org/webworld/child_screen/conf_index.html

¹⁰⁸ Group of specialists on on-line services and democracy: Summary of the replies to the questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services – Secretariat memorandum prepared by the Directorate General of Human Rights, 24 April 2002, www.coe.int/t/e/cyberforum/country_information/Summary_and_analysis/default.asp

⁹⁶ Concluding Observations of the Committee on the Rights of the Child: Austria 07/05/99, CRC/C/15/Add.98, 7 May 1999; Concluding Observations of the Committee on the Rights of the Child: Belgium 07/06/2002, CRC/C/15/Add.178; Concluding Observations of the Committee on the Rights of the Child: Denmark 10/07/2001, CRC/C/15/Add.151; Concluding Observations of the Committee on the Rights of the Child: Finland, 16/10/2000, CRC/C/15/Add.132; Concluding Observations of the Committee on the Rights of the Child: Greece, 01/02/2002, CRC/C/15/Add.170; Concluding Observations of the Committee on the Rights of the Child: Netherlands, 26/10/1999, CRC/C/15/Add.114; Concluding Observations of the Committee on the Rights of the Child: Spain, 07/06/2002, CRC/C/15/Add.185; Concluding Observations of the Committee on the Rights of the Child: Portugal, 06/11/2001, CRC/C/15/Add.162; Concluding Observations of the Committee on the Rights of the Child: Ireland, 04/02/1998, CRC/C/15/Add.85; Concluding Observations of the Committee on the Rights of the Child: Germany, 27/11/1993, CRC/C/15/Add.43; Concluding Observations of the Committee on the Rights of the Child: Luxembourg, 24/06/1998, CRC/C/15/Add.92; Concluding Observations of the Committee on the Rights of the Child: Sweden, 10/05/1999, CRC/C/15/Add.101; Concluding Observations of the Committee on the Rights of the Child: United Kingdom, 09/10/2002, CRC/C/15/Add.188

9.2.1.1 Child Pornography on the Internet on the European Agenda

The specific attention of the European Union to the prevention of child pornography, and particularly to child pornography on the Internet, dates back to October 1996, with the Green Paper on the Protection of minors and human dignity in audio-visual and information services.⁹⁷ For the European Union, it is vital that mechanisms be developed to deal with illegal content and to protect children online.⁹⁸ This position was reaffirmed in the 1996 Commission communication on illegal and harmful content on the Internet.⁹⁹

9.2.1.1.1 Several European Instruments

These documents were followed in February 1997 by a Joint Action paper adopted by the Council concerning action to combat trafficking in human beings and sexual exploitation of children,¹⁰⁰ and in 1998 by article 29 of the Amsterdam Treaty which stresses the relevance of preventing and combating crime, with particular reference to trafficking in human beings and offences against children.

Section III of the Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry human dignity¹⁰¹ invites the Commission to facilitate the networking of the bodies responsible for the definition and implementation of national self-regulation frameworks and the sharing of experience and good practices and to promote multinational co-operation. Additionally, the evaluation of the measures undertaken appears as a key element.

On 25 January 1999, the European Union, by a Decision of the European Parliament and of the Council, adopted a Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. This Action Plan was to cover a period of four years from 1 January 1999

⁹⁷ Green paper on the protection of minors and human dignity in audiovisual and information services, COM (1996) 483, 16 October 1996

⁹⁸ See for more information the Green paper on the protection of minors and human dignity in audiovisual and information services, COM (1996) 483, October 1996; Council Recommendation of 24 September 1998 on the development of the competitiveness of the European Audiovisual and information services industry by promoting a national framework aimed at achieving a comparable and effective level of protection of minors and human dignity (Official Journal L270 of 07.10.1998); Council Decision of 29 May 2000 to combat child pornography on the Internet – 2000/375/JHA; Decision N°276/1999/EC of the European Parliament and the Council of 25 January 1999 adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the regions – creating a safer Information society by improving the Security of Information Infrastructures and Combating Computer-related crime – COM (2000) 890 final

⁹⁹ Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and Harmful content on the Internet, COM(96) 487

¹⁰⁰ Joint Action of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children, JHA/ 97/154

¹⁰¹ Council Recommendation of 24 September 1998 on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, EC/98/560

to 31 December 2002 and was designed to support a range of non-regulatory measures. It had three main thrusts:

- creating a safer environment (creating a European network of hotlines and encouraging self-regulation and codes of conduct),
- developing filtering and rating systems,
- encouraging awareness actions.

The premise was that awareness actions have to be carried out throughout Europe because self-regulation and filter systems would only be successful if Internet users are made aware of the dangers and the possible solutions.

In May 2000, a Council Decision was adopted to combat child pornography on the Internet.¹⁰² The Decision aimed at encouraging the participation of different bodies in the prevention of child pornography on the Internet: institutional bodies, the private sector and civil society.

The Framework Decision¹⁰³, formally adopted in December 2002 by the Council after parliamentary reservations had been lifted, aims to respond to specific requests of the Tampere European Council on 15–16 October 1999 for further initiatives of the European Union in these fields. Where appropriate, the proposal took on board the work reflected at international level in the United Nations Protocol on trafficking in human beings and in the Council of Europe's Convention on Cybercrime¹⁰⁴. Indeed, the European Commission took part in the negotiations on this latter treaty so, although not directly produced by the European Union, it can justifiably be included as part of the strategy set up or endorsed by the European Union in the field of child pornography on the Internet.

Finally, and as noted above, the Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks was initially to cover a short period of four years. But, in 2002, the European Commission adopted a proposal to extend it for two years¹⁰⁵. The aim of the Commission's proposal, now approved, is to introduce new elements and make several adjustments. Most importantly, candidate countries would be associated in ongoing activities, and there would be projects to share experiences and know-how. Another change would be to extend the coverage to new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer and all forms of real time communication. It also seeks to give more attention to other forms of illegal and harmful content on the Internet in addition to child pornography, such as racism and violence, with more active involvement of industry

¹⁰² Council Decision of 29 May 2000 to combat child pornography on the Internet, published in the Official Journal, L138

¹⁰³ Communication from the Commission to the Council and the European Parliament, 'Combating trafficking of human beings and combating sexual exploitation of children and child pornography' – Proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography, COM (2000) 854 final/2

¹⁰⁴ Convention on Cybercrime, ETS n.185, Council of Europe

¹⁰⁵ Communication from the Commission to the Council, the European Parliament, the Economic and social Committee and the Committee of the regions, Proposal for a Decision of the European Parliament and of the Council amending Decision N° 276/1999/EC adopting a Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, COM 2002/152

and more networking among project participants. As the European projects are playing a major role in the field, all these changes should have a real impact on awareness campaigns.

9.2.1.1.2 European projects

In adopting the Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (Action Plan) and its extension for two years, the European Union has strengthened its legislative action. In January 1999, the Action Plan became part of a coherent set of policies at EU level dealing with illegal and harmful content on the Internet. It aims to ensure the implementation of various European Union initiatives and activities concerned with managing undesirable content on the Internet, by supporting non-regulatory initiatives that will promote safer use of the Internet. Concerning awareness and education initiatives, its objectives are to:

- Alert and inform parents and teachers to the issues of illegal and harmful content on the Internet,
- Promote co-operation across Europe and between the actors concerned.

The objectives are to be met through awareness actions, grouped into two Action lines:

- Preparing the ground for awareness actions,
- Encouraging implementation of full-scale awareness actions.

Over the last four years, a number of projects have been at the forefront of the fight against harmful and illegal Internet content through support from the European Commission's Safer Internet Action Plan (IAP): Dot.Safe, Educaunet, CISA, Friendly Internet, Infonet, Once, SafeBorders, Saft, SIFKaL, SUI and SUSI.

These awareness and education initiatives aim to equip educators and parents with the information and resources they need to teach children to stay safe online, to produce and deliver Internet safety information by organisations which the consumer trusts, to promote testing of filtering and rating systems by EU consumer magazines, and to help children to develop an autonomous, responsible attitude in their use of the Internet. This approach is a necessary complement to existing filters, security and classification tools¹⁰⁶.

9.2.1.1.3 Awareness about awareness

a) Four pertinent evaluation reports

It is noteworthy that the present study follows no less than four pertinent evaluation reports at European level submitted in the past four years:

¹⁰⁶ The European Commission agreed in July 2002 that awareness and training are fundamental priorities to tackle Internet Safety.

Promoting safe use of the Internet, how to communicate messages about safe use of the Internet to parents, teachers and children across Europe? (December 1999)¹⁰⁷,

Evaluation Report from the Commission to the Council and the European Parliament (February 2001)¹⁰⁸,

Intermediate evaluation¹⁰⁹ of the implementation of the multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (November 2001)¹¹⁰, and Intermediate evaluation of the Safer Internet Action Plan by BDRC (May 2001)¹¹¹,

Summary of the replies to the questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services (April 2002)¹¹².

The 1999 report on 'Promoting safe use of the Internet' was prepared by the non-profit organisation Childnet International and public relations company Fleishman Hillard, commissioned by the European Commission (DGXIII). The objective of the work was to assess the key messages which would help children stay safe online, and how best to then communicate safety messages effectively to parents, teachers and children across Europe. The research involved: assessing existing Internet safety awareness programmes across Europe, identifying the key messages and styles of communication, developing pilot deliverables and testing these in six countries through focus groups and on online website questionnaire, and then producing recommendations which would support wider awareness actions in the full Safe Use of the Internet Action Plan for 2000 onwards¹¹³.

The February 2001 Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity concluded that 'campaigns for a safer use of the Internet have taken place in most of the

¹⁰⁷ Safe use of the Internet, Promoting safe use of the Internet, How to communicate messages about safe use of the Internet to parents, teachers and children across Europe, Childnet International, Fleishman Hillard, European Commission DGXIII, December 1999

¹⁰⁸ Evaluation Report from the Commission to the Council and the European Parliament on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity – Brussels, 27.02.2001, COM (2001) 106 final

¹⁰⁹ Presentation of the Intermediate evaluation of the Safer Internet Action Plan by BDRC (May 2001)

¹¹⁰ Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the regions – Intermediate evaluation of the implementation of the multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks – Brussels, 23.11.2001, COM (2001) 690 final

¹¹¹ BDRC (Business Development Research Consultants-UK), Intermediate evaluation of the Safer Internet Action Plan conducted for the European Commission – Information society DG, Volumes one & two Final report – 31 May 2001

¹¹² Summary of the replies to the questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services – Secretariat memorandum prepared by the Directorate General of Human Rights – Cyberforum European Council – 24 April 2002, Group of specialists on on-line services and democracy

¹¹³ Some of the findings of this report are referred to in section 2 – Assessment of the effectiveness of preventive measures, Activity 2

Member States¹¹⁴. Several Member States have stressed the importance of schools as the appropriate place for educational measures.’

The BDRC report in 2001 concluded that: ‘the question of regulation of major offences committed against children in cyber-space has been solved. Both European Union and European Council are producing regulations that may or must be incorporated into national legal systems. The development seems to be both unavoidable and welcome.’ And ‘as it will be impossible to control and filter in technological ways due to the whole process of convergence and globalisation...Awareness is the most fruitful and positive part’¹¹⁵.

For the European Parliament, the intermediate evaluation of the Action Plan by the BDRC reveals the following picture. ‘It seems that the EP’s specific recommendations on cost-effectiveness were not taken into account. The European Parliament pointed out quite clearly that traditional information packages are too costly; that new media should be used, and that it is essential to distribute information through industry, for example, by informing journalists of relevant magazines and distributing CD-ROMs with magazines. For the European Parliament, although a lot of projects have been financed, too many goals set out in the original action plan have not yet been reached.’

b) Several meetings

It is equally noteworthy that several evaluation workshops or seminars have been organised in 2002–2003.

A workshop was organised in October 2002 to take stock of lessons learned in protecting and educating children¹¹⁶. The event bridged the end of the first- and the start of the second-generation awareness projects, as well as the current Action Plan and its proposed follow-up, and so took place at a key time.

In preparation for the Safer Internet programme 2003–2004, a hearing was held in Luxembourg on 27 and 28 November 2002. This Safer Internet Forum provided a focal point for discussion at expert level and a platform to drive consensus, inputting conclusions, recommendations, guidelines etc. to relevant national and European channels¹¹⁷. Several working groups answered two main questions proposed by the Commission:

1. What are the key obstacles to Safer Internet awareness in Europe?
2. What defines a good Safer Internet campaign?¹¹⁸

¹¹⁴ Austria, Belgium, Germany, Greece, Spain, Ireland, Netherlands, Luxembourg, Sweden, Finland, United Kingdom

¹¹⁵ BDRC, Intermediate evaluation of the Safer Internet Action Plan conducted for the European Commission, Volume one Final report – 31 May 2001

¹¹⁶ Protecting and educating children in the information society: lessons from European projects – 15 October 2002

¹¹⁷ See the document *eSafe, Directions for 2003–2004 Discussion paper*, eSafe Public hearing 27–28 November 2002

¹¹⁸ The contributions can be found in the website: <http://www.saferinternet.org/resources/e-Safe-consult.asp>

A public consultation on 'Safer Internet plus' was scheduled for Luxembourg on 12 September 2003. The overall objective would continue to be to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end user. In line with this, the programme would focus on the end-user – particularly parents, educators and children. Such a programme would be inspired by the principles of continuity¹¹⁹ and enhancement¹²⁰. The programme will look at the role that different actors concerned (e.g. ISPs, mobile network operators, national regulators, police, software companies, parents, teachers, NGOs dealing with family, children and consumer rights) could play in the fight against illegal, harmful and unwanted content.

9.2.1.1.4 New Perspectives for the Action Plan

During the consultation for the extension of the Action Plan for two years, the Commission explained that it wanted to make several adjustments to the way the Action Plan had been implemented so far. Most importantly, candidate countries would be associated in ongoing activities, and there would be projects to share experiences and know-how. Another change would be to extend attention to other forms of illegal and harmful content on the Internet in addition to child pornography, such as racism and violence, with more active involvement of industry and more networking among project participants.

During the same consultation, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament made several amendments to the Multi-annual Community action plan on promoting safer use of the Internet¹²¹. It opined that more money should be spent on the first two lines (Creating a safer environment and developing filtering and rating systems), and that less money should be spent on encouraging awareness programmes. It further strongly urged that the European Parliament's specific recommendations on cost effectiveness be taken into account.

It was decided that while the initial projects laid the foundations, the forthcoming large-scale projects will span Europe and lead to national nodes focusing awareness at national level. There is a clear need for closer co-ordination and more decentralisation to ensure the intended audience is reached. The intention is to have closer linkage between Action lines on eSafe (a safer environment, filtering and rating systems, awareness and programme support), for example between hotlines and awareness activities, and between rating and self-regulation. Safety is high on the political (and media) agenda in many Member States, and national approaches are deemed to have the best potential effectiveness.

¹¹⁹ Continuity: take account of lessons learned and build on the achievements of the initiatives already funded – such as hotlines, awareness projects, rating and filtering, self-regulation – so as to ensure that their effects continue

¹²⁰ Enhancement: open the programme to new media, to new issues such as 'spam', expand network to accession countries, stimulate a multiplier effect and broaden international outreach.

¹²¹ European Parliament, Committee on citizens' freedoms and rights, Justice and Home affairs, Provisional 2002/0071 (COD) Rev. 6 November 2002 – On the proposal for a European Parliament and Council Decision amending Decision N°276/1999 EC adopting a multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global network, COM (2002) 152-CS – 0141/2002 – 2002/0071 (COD)

Finally, eSafe would differ from its predecessor, the Action Plan, in the following main ways:

- the Action Plan awareness was mostly centred around protection of minors and child pornography; whereas eSafe includes a wider scope of online risks such as racist and xenophobic ideas, extreme violence, hate speech and intolerance.
- the Action Plan was mostly centred around teachers, parents and children, while eSafe takes account of a wider challenge that also includes government, media and industry, especially content providers.
- eSafe will widen its geographical scope, incorporating the accession countries and third countries as well as international organisations,
- eSafe will develop the network of national nodes in order to avoid duplication and increase visibility of Safer Internet actions. Networks have multiplier effects that will also activate local networks to link with national and European networks.

In December 2002, three new awareness projects were launched: Educaunet 2, SafeBorders and SAFT. Although their approach is different, they share the aim common to all the other Safety Awareness projects: to educate children and teenagers to be responsible Internet users.

The major goal of Educaunet 2 is to train teachers and, to a lesser degree, media makers and parents. The overall object is to work with children to sharpen their critical judgement and educate them to systematically seek the source of all information. The methods and tools will be tailored and disseminated in the seven partner countries, namely Austria, Belgium, Denmark, France, Greece, Portugal and the United Kingdom.

SafeBorders aims to establish a cohesive European network to raise awareness of Internet-related risks to protect children and teenagers using the Internet. This European network will take into account cultural and linguistic diversity. The groups targeted include industry, government and media, education institutions and authorities, parents, consumer associations and young people themselves.

SAFT consists of partners from Northern Europe. Their approach to raise awareness is to first 'get the facts' and then use them to pinpoint the exact hotspots for awareness efforts.¹²²

9.2.1.2 Definition of Key Concepts, Legal Framework, Guidelines and Indicators of Effectiveness

This study project seeks to assess the effectiveness of preventive measures enacted throughout the European Union, in the field of child pornography on the Internet, and to contribute to their improvement. In order to achieve this goal, and in line with the methodology developed by Transcrime, three specific objectives were foreseen for the first year:

1. to map preventive measures in place in EU Member States to combat child pornography on the Internet,

¹²² For further information on these projects, see www.saferinternet.org/projects/index.asp ; www.educaunet.org ; www.safer-Internet.net ; www.safeonline.org

2. to evaluate the level of adherence of EU Member States to EU guidelines to combat child pornography on the Internet,
3. to evaluate the effectiveness of the preventive measures in place in EU Member States to combat child pornography on the Internet.

During the first year, the project sought to achieve these objectives through the following two activities:

Activity 1: assessment of the types of preventive measures implemented in the EU in matters of child pornography on the Internet;

Activity 2: assessment of the effectiveness of preventive measures.

9.2.1.2.1 Definition of Key Concepts

Both Transcrime and UNICEF-IRC took on board the official definition of child pornography contained in the Convention on Cybercrime – Council of Europe:

'Child pornography' shall include 'pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct'.

UNICEF-IRC defined *'awareness raising'* as 'any activity intended to bring a particular issue to the attention of a group or groups ('target'), normally with the aim of encouraging attitudinal or behavioural change'. *'Awareness campaign'* was defined as 'a mobilisation for a specific duration, normally using mass communication techniques, with the aim of promoting raised awareness of a particular issue'.

We have defined *'education initiative'* as 'a measure intended to empower or enable a group or groups vis-à-vis a particular issue through the provision of information and/or training'. Within this context, *'sub-national'* refers to the level of government administration immediately below the central level, normally equated with regional government.

'National plan of action' refers, in the context of this research, to 'any plan developed by a country in order to implement the Stockholm Agenda for Action adopted at the First World Congress against the Commercial Sexual Exploitation of children in 1996.' Such Plans are normally drawn up by governmental and child care agencies.

9.2.1.2.2 A Necessarily Evolving Methodology for Conducting Activity 1

a) Identification of guidelines

Although awareness campaigns are mentioned generally in EU instruments, no direct reference is made to specific guidelines concerning the organisation, means and targets of these campaigns. In order to produce guidelines for evaluating the adherence of Member States to European Union legislation in establishing preventive measures against child pornography on the Internet, consideration was therefore given to documents written directly by European Union institutions, and notably the 1996 Green Paper on the protection of minors and human dignity in audiovisual and information services. Due account was also taken of the Council of

Europe Convention on Cybercrime, given that the Council of the European Union subscribed to the principles of this treaty in the common position of 27 May 1999.

In order to obtain the fullest possible picture, UNICEF–IRC considered it crucial to map and analyse not only initiatives taken by governmental actors, but also initiatives taken by non–governmental actors, who play an important role in the field.¹²³

In the light of these general elements and the first analysis of available literature and information, a series of explicit guidelines was developed to take account of both governmental action and that undertaken by others. The two sets of guidelines are set out below.

Guidelines for Governments

General guideline

1. The above–mentioned 1996 Green Paper underlines the importance of the ‘existence of a mechanism to ensure that users of the new electronic services (in particular parents and minors) are aware of the specific risks involved and that they use existing methods of protection effectively’. UNICEF–IRC drew up three different guidelines in this regard:
 - 1.1 Existence of a report on the nature and scale of child pornography on the Internet,
 - 1.2 Existence of a report addressing awareness raising and education initiatives
 - 1.3 Existence of an official commitment of the government to the EU Action Plan for promoting the Safer Use of the Internet.

Awareness (Thematic field)

2. The 1996 Green Paper spoke of the ‘existence of measures to encourage associations and grass roots organizations to become involved in the process of labelling material’, and UNICEF–IRC therefore determined two guidelines on this issue:
 - 2.1 Existence of financial support provided by the government to any non–governmental initiatives for awareness or education,
 - 2.2 Existence of any national–level seminars or congresses regarding child pornography on the Internet organised in the country.
3. The 1996 Green Paper and Council Recommendation of 24 September 1998 on the development of the competitiveness of the European Audiovisual and information services industry by promoting national framework aimed at achieving a comparable and effective level of protection of minors and human dignity (Official Journal L 270 of 07.10.1998) urge ‘ Member States to encourage parental awareness of their responsibility, and encourage consumer associations and individual consumers to become involved in market surveillance (...); and promote action to enable minors to make responsible use of on–line audiovisual

¹²³ First meeting of project partners and the Steering Committee, 19 January 2002

and information services, notably by improving the level of awareness among parents, educators and teachers (...)' UNICEF-IRC reflected this point in one guideline:

- 3.1 Existence of a national awareness campaign regarding child pornography on the Internet directly organised by the government, directed at children and young people, parents, the general public and school teachers.

Education (Thematic field)

4. Council Recommendation of 24 September 1998, cited above, considers that 'the Member States should promote action to enable minors to make responsible use of on-line audiovisual and information services, notably by improving the level of awareness among parents, educators and teachers (...), promote action to facilitate identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places'. UNICEF-IRC split this point into two guidelines:

- 4.1 With respect to child pornography on the Internet, existence of *national* initiatives regarding education of children.
- 4.2 With respect to child pornography on the Internet, existence of *regional* initiatives regarding education of children.

Co-operation (Thematic field)

Council Decision of 29 May 2000 to combat child pornography on the Internet (2000/375/JHA) stipulates that the 'Member States shall examine the possibility of organising regular meetings of competent authorities specialising in combating child pornography on the Internet with a view to promoting general information exchanges, analysis of the situation and the co-ordination of measures in criminal tactics. Each Member State shall notify the General Secretariat of the Council of its organisational unit or units acting as points of contact.' UNICEF-IRC reflected this point in the following guideline:

- 5.1 Existence of organisational unit or units in order to improve co-operation between the different partners

Guidelines for Experts

In order to draw up this set of guidelines, UNICEF-IRC distinguished two different groups:

- the first comprised the five main types of actors potentially involved in promoting education and/or awareness initiatives regarding child pornography on the Internet: NGOs, Internet providers, education authorities, law enforcement agencies and others;
- the second was made up of six target groups: children and young people, parents, general public, school teachers, welfare services and health services.

Awareness and Education (Thematic fields)

Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks notes that ‘consumers should be afforded a high level of protection; whereas the Community should contribute thereto by specific action which supports and supplements the policy pursued by the Member States regarding information for consumers on the safer use of the Internet. An implementation plan will be prepared. The target audience is parents and teachers, and the action will involve industry (Internet service providers, content providers) and multipliers, e.g. consumer associations and the education sector. Actions will be of two types: those focused on teachers and the education sector and those with a broader focus aimed at the general public (parents and children)’.

The Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the regions – creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer-related Crime (COM (2000) 890 final) states that ‘together, industry and law enforcement can raise public awareness on the risks posed by criminals on the Internet.’

Taking account of the above, the guidelines developed by UNICEF-IRC in this sphere were the following:

1. Existence of NGOs involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at:
 - 1.1 – Children and young people
 - 1.2 – Parents
 - 1.3 – General public
 - 1.4 – School teachers
 - 1.5 – Welfare services
 - 1.6 – Health services.
2. Existence of Internet providers involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at:
 - 2.1 – Children and young people
 - 2.2 – Parents
 - 2.3 – General public
 - 2.4 – School teachers
 - 2.5 – Welfare services
 - 2.6 – Health services.
3. Existence of education authorities involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at:
 - 3.1 – Children and young people
 - 3.2 – Parents
 - 3.3 – General public

- 3.4 – School teachers
 - 3.5 – Welfare services
 - 3.6 – Health services.
4. Existence of law enforcement agencies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at:
- 4.1 – Children and young people
 - 4.2 – Parents
 - 4.3 – General public
 - 4.4 – School teachers
 - 4.5 – Welfare services
 - 4.6 – Health services.
5. Existence of other actors involved in promoting education or/and awareness initiatives regarding child pornography on the Internet.
- 5.1 Existence of national projects involved in promoting education or/and awareness initiatives regarding child pornography on the Internet.
 - 5.2 Existence of European Projects involved in promoting education or/and awareness initiatives regarding child pornography on the Internet.
 - 5.3 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at children and young people.
 - 5.4 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at parents.
 - 5.5 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at the general public.
 - 5.6 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at school teachers.
 - 5.7 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at welfare services
 - 5.8 Existence of other bodies involved in promoting education or/and awareness initiatives regarding child pornography on the Internet directed at health services.

b) From one questionnaire to two questionnaires

Once the two sets of guidelines had been prepared, UNICEF–IRC drew up corresponding questionnaires in order to map preventive measures present in each EU Member State. The original intention had been to prepare a single questionnaire to map awareness and educational initiatives, but it was decided to develop two complementary questionnaires following several exchanges with Transcrime, advice

from Ms June Kane of the European Commission¹²⁴ and Mr Nigel Williams of Childnet International¹²⁵, as well as UNICEF–IRC’s own initial experience in attempting to develop a single ‘all-purpose’ questionnaire.

The reasons for this decision were twofold: first, given the potential breadth of this area of intervention and the multiplicity of actors involved, it was considered unlikely that a single respondent – whether within government or civil society – would be in a position to furnish all the necessary information regarding governmental and non-governmental activities in any member state; secondly, the field of education and awareness raising is in constant evolution, and it was considered that a single questionnaire would not necessarily reflect this reality.

The two questionnaires (Chapter 15, Annex 1) were drawn up not only in order to map preventive measures in force in each EU Member State in this area, but also to collect as much information as possible about actors, type of project, means and targets.

Where the expert or civil servant approached felt unable to complete the questionnaire, she/he was asked to recommend other people. Following initial contact with the individual respondents, a follow up email was sent explaining the survey. Identified respondents were contacted further, as necessary, to encourage them to complete the questionnaire.

QUESTIONNAIRE SENT TO GOVERNMENTS

A first questionnaire was sent on 10 May 2002 (Chapter 15, Annex 1) to the most appropriate individuals (e.g. focal points) identified in one or more government ministries in each country of the European Union. In certain countries, it was difficult to identify a single ministry in charge of the question, hence the need in some cases to send questionnaires to more than one. Thus, for example, in Denmark, questionnaires were sent to both the Ministry of Research and the Ministry of Justice.

The questionnaire covered questions divided into three sections.

Information

This section was intended to assess the government’s knowledge about the nature and scale of child pornography on the Internet in the country and preventive measures taken to combat the phenomenon. To this end, it dealt specifically with declarations and with governmental reports, including reports to the UN Committee on the Rights of the Child.

¹²⁴ ‘In my experience, one of the problems we face (especially in Europe) is that sectors work far too often in isolation and don’t know what other sectors are doing. Would it not be better to have a series of shorter questionnaires targeted at the specific sectors (i.e. a government-specific questionnaire to send to governments, an NGO questionnaire to send to major NGOs, etc...)

¹²⁵ Nigel Williams : ‘because few children and parents see such material, there is limited need for awareness programmes about the child pornography material itself. There is a real need to look at professional awareness of these issues among police and social workers’.

‘Most education and awareness programmes are about more general Internet safety questions.

Of course, hotlines need to publicise their work but that is different from publicising about child pornography on the Internet. There is a real need to look at professional awareness of these issues among police and social workers but that too is a different question.’

Involvement

This section sought to assess the government's involvement in implementing preventive measures to combat child pornography on the Internet, and specifically awareness and educational initiatives. To this end, it dealt specifically with public policy, a National Plan of Action on the sexual exploitation of children (in the context of follow-up to the 1996 Stockholm Congress) addressing education and awareness raising regarding child pornography on the Internet, commitment to the EU Action Plan for promoting the Safer Use of the Internet, and financial support to any non-governmental initiatives for awareness raising or education.

Commitment

This section was designed to assess the government's commitment to implementing preventive measures to combat child pornography on the Internet, i.e. the concrete implementation of awareness campaigns and education initiatives. These initiatives may be trans-national, with a significant component in the country, national or sub-national.

Questionnaires were sent to thirty-one potential respondents. Disappointingly, only six replies were received – from the Governments of Austria, Denmark, Finland, Germany,

Sweden and the United Kingdom – despite several attempts to secure complete data from each non-responding government source¹²⁶.

QUESTIONNAIRE SENT TO EXPERTS

The second questionnaire was sent, on the same date, to the identified experts in each country of the European Union (usually working within an academic or NGO context). For some countries, the questionnaires were sent to more than one expert. The questionnaire covered questions divided into two sections:

Existence of different actors

This section was intended to assess various actors' commitment to implementing preventive measures to combat child pornography on the Internet, and specifically awareness and educational initiatives. To this end, it dealt specifically with six identified groups of actors: NGOs, Internet providers, education authorities, law enforcement agencies, media and other bodies; and asked several questions: Who is committed, who is the target of the education and awareness raising, what are the means employed?

Co-ordination of all the initiatives

This section sought to assess the level of co-ordination and co-operation among the various actors. To this end, it dealt specifically with national committees, co-ordinated activities and national-level seminars or congresses regarding child pornography on the Internet.

Fifty-two questionnaires were sent out to the experts and nineteen replies were received. Thus, for some countries, two or even three replies were received, giving relatively good insight into the situation there. Responses were as follows: Austria,

¹²⁶ One explanation for this situation could be the number of questionnaires for surveys in this field sent to governments in the space of three years, as noted in the introduction to this report.

Belgium (2), France, Finland, Greece (2), Ireland, Italy (3), Netherlands (2), Portugal (2), Spain and United Kingdom (3).

c) Level of adherence and lessons learned about the methodology

The results of the first stage of the project – ‘Mapping the preventive measures’ – were initially intended to be presented in the form of tables indicating percentage of adherence of EU Member States to EU guidelines on the prevention of child pornography on the Internet. It was assumed that ‘The higher this index, the higher the adherence of EU Member states to EU guidelines on the prevention of child pornography on the Internet.’ In order to calculate this index the adherence of each EU Member State to each EU guideline was investigated. The answer ‘Yes’ was assigned in case of adherence of a Member State to a given EU guideline, while the answer ‘No’ was assigned in case of non-adherence.

The second step involved assigning respectively the value ‘1’ to each answer ‘Yes’ and the value ‘0’ to each answer ‘No’ in relation to the existence of a given guideline in the Member State’s legislation (Chapter 15, Annex 2).

For mapping awareness campaigns, however, it became apparent to UNICEF-IRC that the results could not be reduced to one quantitative matrix for each questionnaire without oversimplifying the results, and that the methodology initially agreed for the project as a whole would be inadequate as an analytical basis for assessing adherence in the sphere of awareness initiatives.

First, methodology based on a matrix of binary values does not permit responses to be weighted. In this way, quantitative matrices certainly hide as much as they reveal. In particular, this seems the case with the responses to the expert questionnaire. It is clearly not enough to say ‘yes, there is an NGO involved in these issues’ – the point is how effective this NGO is, what its awareness raising strategies are, etc... Equally, a country with ten well-organised NGOs, and another with just one small home-based operation, both fall into the same category according to the classification of such a quantitative matrix. At the same time, developing a more detailed, systematic approach requires time, funds and technical means that were not available in the context of this project.

Second, the methodology does not take account of incomplete responses and ‘don’t know’. We would consider ‘don’t know’ to be a valid answer, indicating as it does that government officials or NGOs are actually unaware of whether or not education and awareness-raising initiatives exist in their own country, a fact telling in itself.

Third, the number and variety of actors potentially involved in awareness and education initiatives in any given country – a reality fully realised only during the course of the project – results in a situation of complexity and richness which cannot be reflected in a simple matrix.

Fourth, the changing nature of awareness campaigns and their duration cannot be taken into account using a simple matrix. Additionally, a simple quantitative ‘output’ without consideration of the target audience/means of dissemination and the nature of the message itself is clearly not sufficient in this case.

Finally, adherence to EU-guidelines in the field that UNICEF-IRC was to investigate is not necessarily the outcome of EU-led initiatives, something recognised by the Commission of the European Union itself in various instruments. Calculating a

percentage of adherence suggests a false linkage. Thus, other international instruments may guide national policies in this area, national media reports may provoke action, and a wide range of independent, spontaneous initiatives may exist at the local level¹²⁷. For example, UNICEF–IRC has collected information on the observations of the UN Committee on the Rights of the Child and the National Plan of Action on sexual exploitation of children, adopted by numerous governments after the Stockholm Congress in 1996. Given that the matrix does not allow for the incorporation of such data, it inevitably risks distorting national pictures. For this reason, UNICEF–IRC also collected and analysed information on government responses to sexual exploitation of children after the Stockholm Congress in 1996.

Despite these recognised limitations, UNICEF–IRC secured as much quantitative data as possible, and in September 2002 submitted two quantitative matrices – one for governmental initiatives and one for other actors' initiatives (Chapter 15, Annex 3).

d) Mapping of preventive measures and postponements of the report

In June 2002, Transcrime requested postponement of the deadline for delivering the intermediate report. The new deadline for the delivery of the report was the end of October 2002. The postponement of the report was motivated by two major factors:

- the need to devote more time to the first phase of the development of the project, viz. the mapping of preventive measures against child pornography on the Internet, crucial for the subsequent development of the project;
- the involvement of some organisations, such as INHOFE, in the project had taken more time than originally expected, and this had delayed the execution of the project.

Then, in November 2002, a slowdown of the project until September 2003 was agreed between Transcrime and the European Commission. This implied that the final report on Activity 1 (mapping of preventive measures) and Activity 2 (effectiveness of preventive measures undertaken) was expected for September 2003.

For UNICEF–IRC, these postponements clearly made it necessary to update the results of mapping. Account needed to be taken of the rapid evolution of awareness and educational initiatives between June 2002 and June 2003, and UNICEF–IRC was convinced that only a clear and updated picture of these measures, of their organisation and functioning, would make it possible to select appropriate effectiveness indicators.

¹²⁷ It is interesting to note that the partial impact of EU instruments and the role of other instruments is explicitly recognised by the European Commission itself in the proposal for a Framework Decision on Combating the Sexual Exploitation of children and child pornography (2001), in which it draws attention to the importance of 'work performed by international organisations'.

9.2.1.2.3 Methodology in order to conduct Activity 2

a) Main assumption

The general goal of all preventive measures, including awareness and educational initiatives, related to child pornography on the Internet is to contribute to the reduction of the overall level of pornographic material circulating on the Internet. However, it is not presently possible to determine how much awareness and educational initiatives contribute to this achievement, given the lack of consistent and on-going monitoring. Therefore, the main assumption is that the better and more effective the process of production of awareness and educational measures, the better the achievement will be.

For UNICEF-IRC, this notwithstanding, and given the global and borderless architecture of the Internet, effective preventive measures would be those that can be adapted to the specific nature of the Internet. These would constitute the measures with the greatest potential for reaching as many children as possible and making them and their family aware of, and protected from, the risks of exposure to child pornography via that medium.

b) Identification of indicators of effectiveness

Four indicators of effectiveness of the preventive measures in each area of intervention (Annex 4) were identified:

1. Multiplicity of actors involved,
2. Multiplicity of means used,
3. Coverage and outreach,
4. Sustainability of projects.

These four complementary indicators were extrapolated in the light of research and reports analysed regarding the nature of the Internet as a new and specific means of communication – in other words, the tools for action have to be adapted to the Internet world. Thus, as noted by the Bertelsmann Foundation, ‘for a public response to be effective, it must be integrated, systematic and dynamic, sensitive to public needs and national differences within a framework that encourages robust communication. Only such a systematic approach – bringing technological potential together with the energies and capacities of government, the Internet industry and the citizens – has the promise of successes.¹²⁸ And many of the various actors support this point of view when developing awareness and education initiatives.

MULTIPLICITY OF ACTORS INVOLVED

As also underlined by the Bertelsmann Foundation, ‘no single approach, relying on one form or set of actors, can provide a solution to content concerns in the changing and shifting environment that is the Internet’.¹²⁹ The report on Promoting

¹²⁸ Self-Regulation of Internet Content, Bertelsmann Foundation, Gütersloh, 1999

¹²⁹ *ibid.*

Safe Use of the Internet¹³⁰ states that 'from researching existing safety awareness programmes, it was clear that the most successful were ones which involved partners from all sectors, e.g. government, education, industry, child welfare, parents groups, etc...'. The research also confirms the fact that industry involvement in safety awareness is crucial, as Internet companies have good communication channels to reach their customers and can profile the issue.

MULTIPLICITY OF MEANS USED

Existing research¹³¹ shows that 'for an Internet safety awareness campaign to be effective, online and off-line elements need to be integrated and complementary. Furthermore, awareness campaigns need to be imaginative and capture the user's attention and differentiate themselves from the saturation of media messages'. Although a website is crucial, its production must not be seen as the sole solution. As stated by the Infonet project, 'a good web site will not be sufficient, especially as we know that many parents, teachers and children still do not have access to the Internet'¹³².

Regarding the material prepared and the message, the evaluation shows not surprisingly that as many means of communication as possible should be used if outreach to the public is to be maximised. These means include: printed material for presentations, online published material, practical guides for parents, teachers and social workers, practical guides for children and students, leaflets, CD Roms, websites, information letters to parents, teachers, parents' organisations, websites, research studies carried out for government organisations, TV appearances, radio, newspaper articles and posters. Furthermore, safety messages have to be communicated clearly and targeted at different audiences. Childnet International and Fleishman Hillard, in 1999, 'urge the development of cross-sectoral campaigns and urge those undertaking awareness campaigns to use different deliverables to reach different audiences'.¹³³

Other research has shown in addition a preference for images and styles of safety tips that emphasise the positive and help empower children to take responsibility themselves.

COVERAGE AND OUTREACH

The research brought to light some excellent global Internet awareness programmes as well as some smaller-scale Internet safety initiatives for specific groups – adults, children, teachers at local or regional level – and a few European-funded programmes in EU Member States. There are also some very good examples of individual projects. UNICEF-IRC takes on board the idea that there is a need for a

¹³⁰ Safe use of the Internet, Promoting safe use of the Internet, How to communicate messages about Safe use of the Internet to parents, teachers and children across Europe, Childnet International, Fleishman Hillard, December 1999

¹³¹ See the list of evaluation projects above

¹³² Final Report Infonet project, November 2001

¹³³ Safe use of the Internet, Promoting safe use of the Internet, How to communicate messages about Safe use of the Internet to parents, teachers and children across Europe, Childnet International, Fleishman Hillard, December 1999

simultaneous mix of local, regional, national and European awareness and educational initiatives.

SUSTAINABILITY

This is probably the most difficult challenge: results achieved need to be long lasting or permanent, and the research therefore tried to ascertain whether achievements to date would still be in place once the Action itself has ended. It is clearly desirable for projects to have a sustained impact after funding has ceased. Thus, a website is crucial, but it needs to be updated constantly. However good an educational initiative may be, it needs to be reproduced every year to inform the new intake of pupils.

Childnet International and Fleishman Hillard, in 1999, stated that 'it is crucial that Internet safety is integrated with the fuller net literacy training of young people so that as well as learning how to use the Internet, evaluate the reliability of information, knowing how to publish and exploit the medium, children also know how to keep safe'.¹³⁴

As any evaluation of effectiveness should include data derived from primary sources – i.e. replies to the questionnaire – and from information gathered from websites, written documents, documentary research in the legal and practical fields, publicly available official documents, and scans of relevant Internet sites, the conclusions of the present report are a synthesis of all these materials.

9.2.2 Section B: Presentation of the Findings

9.2.2.1 Assessment of the Types of Preventive Measures Implemented in the EU – Activity 1

The information obtained through analysis of the questionnaires, together with supplementary data from analysis of existing secondary sources, is summarised in a series of synoptic tables, which are available in Annex 3 of this report. Much information can be usefully derived from these matrices and, furthermore, the very absence of information is, in itself, instructive.

The matrices outline the preventive measures reportedly in place in the area of education and awareness in each EU Member State. From these tables, we can identify:

- Actions undertaken by the governments according to three main categories: information, involvement and commitment,
- Actions undertaken by other actors: NGOs, Internet providers, education authorities, law enforcement agencies, media and other bodies.

The tables indicate that the measures in place in EU Member States to combat child pornography on the Internet have three main characteristics:

Heterogeneity of the measures taken by the Member States (*1.1.1 Adherence of EU Member states to EU guidelines*),

¹³⁴ *ibid.*

Multiplication of actors developing awareness initiatives in the Member States
(1.1.2 Adherence of different actors to EU guidelines),

High impact of European projects (1.1.3 Impact of European projects).

Finally, findings also highlight the limitations of the mapping exercise. These are twofold in nature: technological and cultural: country-specific cultural, linguistic and social-economic factors can impact on the content and use of the Internet (1.2: limitations of the mapping exercise).

9.2.2.1.1 Mapping of the measures in place in EU Member States against child pornography on the Internet

A) Adherence of EU Member States to EU guidelines: Heterogeneity of the measures taken Information

All governments display some degree of knowledge about the nature and scale of child pornography on the Internet in the country. All acknowledge the dangers of the Internet but none considers that these may have slowed down its development.

Whereas in seven countries a report on the issue has been prepared by the government itself¹³⁵, in others reports were the work of university faculties or NGOs¹³⁶, sometimes financed by the European Union¹³⁷. The majority of these reports were completed in 2000–2001, except for France and Sweden where they are expected for 2003–2004.

Most reports are about more general Internet safety issues or more general sexual exploitation of children questions, and are viewed also as information sources for professionals and/or the public. Reports may contain statistics and/or guidelines, and proposals for future initiatives.

From perusal of the Concluding Observations of the UN Committee on the Rights of the Child, which regularly requests that measures be taken to protect children from harmful images shown on the Internet, it is clear that all countries are submitted to a high and regular pressure concerning the production of a report¹³⁸ and the adoption of preventive measures.

INVOLVEMENT

Most countries state that they are involved in the implementation of preventive measures to combat child pornography on the Internet, especially awareness and educational initiatives. Resolutions and recommendations have been made concerning 'Child pornography on the Internet, violence in the media'¹³⁹, and consultations have been initiated with various authorities, as in Denmark. Some

¹³⁵ Austria, Denmark, Finland, France, Ireland, Netherlands, Italy

¹³⁶ Belgium, Germany, Greece, UK

¹³⁷ Greece, Austria

¹³⁸ See in the bibliography the references of 'Concluding observations of the Committee on the rights of the child'.

¹³⁹ Austria, Ireland

countries have developed official websites for reporting illicit websites and for being informed about the dangers of Internet use¹⁴⁰; others have created a working group¹⁴¹.

It seems, however, that few governments have attributed financial support to non-governmental initiatives for awareness raising or education¹⁴². At the same time, it should not be forgotten that a significant proportion of the respondents recognise that they do not know if the government is providing financial support in this field.

In ten countries, national-level seminars or congresses regarding, directly or indirectly, child pornography on the Internet have been organised¹⁴³. But these seminars rarely address awareness initiatives on child pornography alone. For example, in France the Ministry of Employment has organised the 'generalist' *Rencontres du Net*. In January 2001, Red Barnet and Tele2, one of the major Danish ISPs, hosted the first major national conference where policy-makers and other key stakeholders discussed 'The challenges of Internet safety for children'. The title of the International Summit of Thessalonika in Greece (March 2001) was 'Children and media'. In Naples, Italy (November 2001) there was a conference on *Minori in Internet*, and a conference entitled

'Casting a wider net: integrating research and policy on the social impacts of the Internet' was held in Oxford in September 2002.

COMMITMENT

This section is intended to assess the government's commitment to implementing preventive measures to combat child pornography on the Internet. It deals with the concrete implementation of awareness campaigns and education initiatives.

Campaigns for a safer use of the Internet have taken place in at least eight of the Member States¹⁴⁴. Several have been only partial. In Belgium, the '*Cliquer futé*' campaign targets only the French-speaking community and, within this community, only children aged 6 to 12 years. Other countries, such as France, Germany and Italy, have launched limited campaigns when setting up online information web-sites¹⁴⁵. Nonetheless, it seems that at least two countries¹⁴⁶ have undertaken global national awareness campaigns. In the Netherlands, several ministries and a number of private organisations and companies have started an ongoing awareness campaign on how to use the Internet safely, especially in schools. And in the UK, the Home Office has set aside £1.5 million for a national awareness campaign using a range of media (cinema, commercial radio stations and magazines) to educate children on the issue.

¹⁴⁰ France, Germany, Luxemburg

¹⁴¹ France, Portugal, Spain

¹⁴² Austria, Denmark, Finland, Germany, Sweden, Netherlands,

¹⁴³ Austria, Belgium, Denmark, Finland, France, Ireland, Netherlands, Spain, Sweden, UK

¹⁴⁴ Belgium, Denmark, France, Germany, Ireland, Italy, Netherlands, and UK

¹⁴⁵ France and the web-site www.social.gouv.fr/famille-enfance/fam_lign/; Germany and the website: www.sicherheit-im-internet.de; Italy and Ciclope

¹⁴⁶ The Netherlands and the UK

Respondents to the questionnaire noted national or regional initiatives regarding education of children as being in place in ten countries, but the scale of these initiatives varies widely¹⁴⁷ (see below under Existence of Different Actors).

b) Adherence of other actors to EU guidelines: Proliferation of initiatives undertaken

The heterogeneity of the measures taken by governments should not necessarily be taken to mean that certain countries are inactive in this field. Already, as underlined by the Bertelsmann Foundation, 'no single approach, relying on one form or set of actors, can provide a solution to content concerns in the changing and shifting environment that is the Internet'. Many different types of actors subscribe to this point of view in developing awareness and education initiatives

Bearing this in mind, this section is intended to assess these actors' commitment to implementing preventive measures to combat child pornography on the Internet – specifically awareness and educational initiatives – and to evaluate co-ordination and co-operation among these actors.

EXISTENCE OF DIFFERENT ACTORS

This section deals specifically with five identified groups of actors: NGOs, Internet providers, education authorities, law enforcement agencies and other bodies. It looks at who is committed, who is the target of the education and awareness raising, and what means are used.

A review of these actors highlights a variety of different approaches to the problem of illegal and harmful use of the Internet. Some actors have followed government initiatives where they exist, others have encouraged a self-regulatory approach by the industry, and yet others come from the child welfare sector and are well versed in the promotion of awareness projects¹⁴⁸.

In almost all countries, one or several NGOs are involved in promoting education and/or awareness initiatives. Some respondents noted that there are so many activities in this area that it is difficult to estimate numbers¹⁴⁹, whereas in countries like Greece, Ireland and Denmark it was difficult to find more than one NGO developing awareness initiatives. All these organisations have reportedly paid increasing attention to these initiatives since 2001, however.

Since the main targets of these initiatives are children and young people, it seems to be an *a priori* aim to empower end-users by giving them the necessary information to allow them to make responsible decisions. The second target groups are parents and the general public. It can be noted that many of these initiatives are

¹⁴⁷ Austria, Belgium, Finland, France, Ireland, Italy, Netherlands, Spain, Sweden and UK

¹⁴⁸ The Infonet project has determined two different groups of associations: horizontal and vertical. Horizontal associations are those with a more general and neutral character; they cover all aspects of the use of Internet within the different segments of society. Vertical associations are dedicated to a specific activity, with well-defined views about the role of the Internet in society and with very concrete lines of action. They might have a direct influence in issues concerning education and the spread of the use of Internet among society. *Final Report Infonet project*, November 2001

¹⁴⁹ Finland, UK, Sweden, Netherlands

of a regional/local character and are generally linked with and/or funded by the EU Safer Internet Plan.

Nine countries confirm the existence of Internet providers involved in promoting education and/or awareness initiatives¹⁵⁰. Internet providers frequently act via the platforms of various partners and then share with them the same targets and means. While some hotlines limit their advertising activities to promoting the hotline itself, others are also involved in more general awareness campaigns, often with the co-operation of the funding institutions. In many cases, the ISPs are the hotline funding institution. As stated in the Evaluation Report from the Commission in 2001, the efficiency of hotlines could be increased¹⁵¹ by making their existence better known to Internet users. However, major campaigns have taken place in only five Member States¹⁵² and limited information has been provided in just two others¹⁵³. One Member State currently envisages launching an information campaign¹⁵⁴.

In all, thirteen countries are said to have education authorities involved in awareness and education initiatives.¹⁵⁵ These campaigns may be launched by the Ministry of Education or by local or regional education authorities, often in the framework of European Projects (Dot.safe projects, Educaunet, SIFKaL, ONCE, Friendly Internet...). In recent years, considerable energy has been devoted to the preparation of information papers¹⁵⁶, materials for workshops and conferences, campaign materials such as safety guides for teachers, posters for schools, websites, boomerang cards, etc. These materials have been conceived for different age groups: 6–10, 10–14 and 15–18 year-old pupils, although it is important to stress that the core targets are 12–16 year-olds. Several countries have conducted studies with children¹⁵⁷ and young people in order to collect information about the way they use the Internet.

While the main objective of these campaigns is to make children responsible users¹⁵⁸, the whole range of grown-ups who are involved with children's education and upbringing are also sometimes targeted¹⁵⁹: teachers, parents, adult educators, etc.

¹⁵⁰ Austria, Belgium, France, Italy, Ireland, Netherlands, Spain, Sweden, UK

¹⁵¹ Evaluation Report from the Commission to the Council and the European Parliament on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity – Brussels, 27.02.2001, COM (2001^o 106 final)

¹⁵² Denmark, Ireland, Netherlands, Finland, United Kingdom

¹⁵³ Germany, Sweden

¹⁵⁴ Spain

¹⁵⁵ Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Portugal, Sweden and UK

¹⁵⁶ For example, Childnet International and Fleishman Hillard analysed what sort of messages needed to be given to parents and children about safer use of the Internet and how best these should be presented. The results include a user guide in 11 languages. <http://www.netaware.org/gb/website.html>

¹⁵⁷ Austria, Greece, Ireland, UK

¹⁵⁸ Austria, Denmark, France, Belgium, Ireland, Italy, Netherlands, UK

¹⁵⁹ Denmark, France, Ireland, Netherlands, UK

Few experts provided information about the existence of law enforcement agencies involved in promoting education or/and awareness initiatives¹⁶⁰, though a significant number recognised that they simply did not know whether or not such activities were taking place. Those that were mentioned are generally joint initiatives among various ministries and linked with an official website for reporting illicit websites and receiving legal information.

Very few media groups are said to be engaged in awareness or education initiatives as such, but media attention to cases of paedophilia can have a significant impact on public opinion. Many discussions and round tables have taken place on this issue with wide media coverage. In Spain, the Infonet partners were able to secure considerable media attention to their project through a press conference: several newspaper and web articles were published and the partners were invited to appear in several TV news programmes. In Italy, however, the partners were less fortunate: the media were seemingly not prepared to publicise these kinds of campaigns.

Certain other actors are also involved in promoting education or/and awareness initiatives: examples are the *Institut National des consommateurs* (France) and E.K.A.T.O. (Greece). The Bertelsmann Foundation (Germany), the Foundation Safer Internet (Netherlands) and the Internet Watch Foundation (UK) are dealing with the security of young Internet users and are working closely with several partners in the field.

Finally, although the main tasks of Internet hotlines are to enable users to find all necessary information regarding national legislation, and to receive reports on suspected child pornography material publicly available on the Internet, they are also involved in more general awareness campaigns¹⁶¹.

CO-ORDINATION OF INITIATIVES

This section is intended to assess the degree of co-ordination and co-operation between the different actors.

Eight countries seem to have some form of co-ordination of awareness and education initiatives, but the nature of this co-ordination is quite different from one country to another¹⁶². It may be an Informal Forum for discussion, as in Austria, where ministries, authorities, industries, consumer associations and NGOs participate; or an official structure like the Internet Advisory Board (Ireland) or the Internet Rights Forum (France). In Sweden, it takes the form of a Reference Group composed of non-governmental partners that exchange up-to-date information; in Belgium, there is a Network of partners including ISPA, the Ministry of Justice, the Ministry of Telecommunications and the Federal Computer Crime Unit.

Probably the most effective types of co-operation and co-ordination structures are to be found in the Netherlands and the UK. In the latter, a Task Force on child protection on the Internet, linked with the Strategy Group in the Department of Education, brings together representatives of several actors and facilitates the organisation of public awareness campaigns.

¹⁶⁰ Belgium, Denmark, France, Germany Netherlands and UK

¹⁶¹ INHOPE Association of Internet Hotlines Providers in Europe, first Report, INHOPE, May 2002

¹⁶² Austria, Belgium, Denmark, France, Germany, Ireland, Netherlands, UK

c) Impact of European projects

The Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks came into effect in January 1999 and is part of a coherent set of policies at EU level dealing with illegal and harmful content on the Internet. It aims to ensure the implementation of various European Union initiatives and activities concerned with managing undesirable content on the Internet. It is noteworthy that while mapping national preventive measures in place in EU Member States, UNICEF-IRC has found at least one European project involved in each country, with the apparent exception of Luxembourg.

EUROPEAN PROJECTS

Over the last four years, a number of projects have been at the forefront of the fight against harmful and illegal Internet content through support from the European Commission's Safer Internet Action Plan (IAP): Dot.Safe, Educaunet, CISA, Friendly Internet, Infonet, Once, SafeBorders, Saft, SIFKaL, SUI and SUSI.

Projects/ Country	Budget (.000€)	Austria	Belgium	Denmark	Finland	France	Germany	Greece	Ireland	Italy	Luxembourg	The Netherlands	Portugal	Spain	Swede	UK
sDot.Safe	1.930				X	X			X	X						X
CISA	225	X	X			X		X		X			X	X		
Educaunet	495		X			X										
Friendly Internet	215	X								X					X	
Infonet	240									X				X		
Once	695		X					X	X							
Safeborders	1.807					X		X		X				X		X
Saft	1.370			X					X						X	
SIFKaL	1400						X	X						X		X
SUI	275	X			X								X	X		
SUSI	295												X	X		X
Total Projects		3	3	1	2	4	1	4	3	5		2	1	7	2	4

European Projects funded by the EU Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (1999-2002)

Dot.safe

This is a pilot project supported by education and technology bodies across Europe. It aims to equip educators and parents with the information and resources they need to teach children to stay safe online. There are four principal areas of work:

1. Identifying audiences, resources and approaches, identifying types of Internet users among teachers, auditing their concerns, collating resources, solutions and effective practices to raise awareness of Internet safety in schools.
2. Developing new materials, adapting those that exist, and identifying technical solutions.
3. Testing and evaluating.
4. Developing detailed scalable plans

CISA

Seeing consumer and family organisations as ideal intermediaries to educate both parents and children, the project centres on the production and delivery of Internet safety information by organisations which the consumer trusts. CISA also seeks to promote testing of filtering and rating systems by EU consumer magazines in Spain, Belgium, Italy and Portugal.

Educaunet

The Educaunet project aims to help children to develop an autonomous, responsible attitude in their use of the Internet as a necessary complement to existing filters, security and classification tools. The project sets out to help parents and education professionals get a better command of the advantages and risks of the Internet, and to produce and publish an integrated package of tools and media to help adults and teachers in this education process.

Friendly Internet

The project aims to achieve wider and safer use of the net by promoting the role of parents, teachers and social workers. The project encourages co-operation among key school actors, families, ISPs, associations and institutions by carrying out joint initiatives in the field of awareness raising campaigns. The pilot phase has involved secondary and high schools in Italy, Sweden and Austria.

Infonet

The aim of this project is to prepare awareness campaigns in Italy and Spain. The target audience comprises Internet end users and Internet service and content providers. Major civil rights groups, associations and media have been consulted to obtain the right messages to be included in the campaigns. Two versions of each kind of information material have been prepared: one aimed at end users and one with more technical details aimed at ISPs, content providers and Internet IT developers. Multiplier organisations have been identified for each kind of user in the target audience in order to distribute the information material.

ONCE

This project seeks to involve children and teenagers in the process of formulating and developing on-line safety guidelines. It will prepare the ground for awareness actions: creation of a website and registration thereof with search engines; development of a user-friendly package; participation in a process of information exchange with the other IAP projects.

SafeBorders

SafeBorders is to establish a cohesive European Network to promote and support awareness aimed at the protection of children and teenagers using the Internet. In its current phase, SafeBorders targets directly five partner countries, viz. Germany, Greece, Italy, Spain and the UK. The national-level awareness campaigns address the perceived shortage of information regarding the safety of minors on the Internet and seek to empower parents, teachers, children, consumers and other relevant target groups.

SAFT

This Consortium sets out to teach children and teenagers to be responsible Internet users and to diminish risk behaviour in these groups. The project also seeks to empower parents and educators to help children reach this goal, as well as to raise awareness within the Internet industry, in order to make it more responsible. The final objective of the project is to raise the question of awareness on national levels of discussion in the project countries.

SIFKaL

The central objective of the SIFKaL project is to develop and disseminate information and recommendations about the educational and socially relevant potential of the Internet, by means of a permanent virtual site that is multilingual and in a different format for each of the four target groups: parents, teachers, librarians and local authorities. Four case studies have been carried out in educational and socially relevant contexts in order to find out 'what exactly does safer Internet mean?'

SUI

This project informs parents, teachers and educational staff of the benefits and dangers of the Internet. Information is given on the nature of the Internet, technical provisions for guided use and methods of dealing with incidents resulting from illegal or harmful content. Awareness methods have included dissemination of printed information, seminars for teachers, information events for parents, workshops for children/pupils, electronic publishing and various ad hoc services via the Internet: Helpline, advice for selective proxies and organised events for children/pupils.

SUSI

SUSI is a consortium of public and private partners from UK, Spain, Netherlands and Ireland. It has created trans-national sources of support for parents and teachers, providing Internet awareness information and usage advice (both online and offline) in forms that are easy to access, use and comprehend. The project has developed active dissemination of the safe-use messages through means such as face-to-face meetings, pupil-to-home delivery, and direct mail.

TAKING STOCK OF LESSONS LEARNED

A workshop was organised in October 2002 to take stock of lessons learned in protecting and educating children, during the implementation of the Action Plan¹⁶³. The meeting was premised on the supposition that 'While the initial projects laid the foundations (1999-2002), the forthcoming large-scale projects will span Europe and lead to national nodes focusing awareness at national level. Therefore there is a clear need for closer co-ordination and more decentralisation to ensure the intended audience is reached. It is the intention to have closer linkage between Action lines on eSafe (a safer environment, filtering and rating systems, awareness and programme support), for example between hotlines and awareness activities, and between rating and self-regulation. With safety riding high on the political (and media) agenda in many Member States, national approaches will prove most effective'.

Several findings of the workshop are worth mentioning in the context of the present report. First, a number of lacunae were noted. For example, in Greece, there is reportedly a lack of knowledge about the Internet among parents and teachers – their main sources of information are traditional mass media. Libraries are having to balance the need for privacy and autonomy versus controls over access and use by young people. In Spain, lack of co-operation among socio-educational institutions involved in shaping strategy was noted.

Among other concerns highlighted were: the fear that awareness campaigns may inadvertently 'market' the dangers they set out to combat; parents' need for simple answers whereas the target audience is complex and does not just break down into differences in age; and the challenge of keeping up with the constantly changing technology.

It was pointed out that traditional approaches should not be neglected, as they can strengthen ties between the home and school and engage all those involved. Ties with commercial companies and the education services can lend credibility to efforts. It was considered important, however, that efforts complement each other and be seen to be working together.

The work of these awareness projects has brought to light the high level of demand for information on the part of parents, pupils and teachers. But whereas a range of innovative ideas was presented (awareness messages in airline magazines, on postcards and on milk cartons to ensure such messages reach every household...), with the onset of new technologies, new actions are needed combining both education and guidance, and protection through filters and safe sites, for example.

¹⁶³ Protecting and educating children in the information society: lessons from European projects – 15 October 2002

It was clear from the project presentations and discussion that followed that education was important to better understand the dangers and the messages being sent. Similarly, the concept of responsibility and citizenship are important to engage the young. Self-regulation and codes of conduct also have key roles in tackling the changes in scope of activities online. The Internet is complex and different users enjoy it differently.

Awareness raisers need to adapt information to every target group to maximise its outreach.¹⁶⁴

9.2.2.1.2 Limitations of the mapping exercise

Although the problem of child pornography on the Internet seems to be very real, its magnitude varies according to the demographic and socio-economic reality of each country as well as to the latter's historical and cultural context. The overall national situation is reflected in the resources potentially and actually made available. The counter-measures too will therefore be relative.

a) Level of Internet Penetration in EU Member States

It seems reasonable to assume that the larger the percentage of online users, the greater the chance that there will be a significant proportion of users who are less sophisticated in terms of their computer fluency and their general level of education. In turn this will have some impact on, for example, judgements about the ability of parents to use filtering software and to understand some forms of 'awareness' advice.¹⁶⁵

In this regard, as shown in *Table 1* opposite, while the overall level of penetration in the Member States stands at 33%, this figure masks very significant national differences, from Greece with a rate of 13% to Sweden at 51%. The four most populous EU countries – France, Germany, Italy and UK – which comprise 68.3% of total EU population and a similar percentage (just over 71%) of the region's online users, are all in the middle range for penetration (from 28% to 40%).

These variations in general penetration are compounded by the differences in the proportion of under-17 users and the amount of time they spend on-line. The results of the 5-country survey conducted in 2002 and summarised in *Table 2* show, for example, that with equivalent percentages of under-17 users, young people in the UK would seem to spend almost 80% more time on the Internet than their Danish peers, yet only half the time, on average, of the far smaller German contingent. Together, these factors set in context the number, size and nature of awareness initiatives taken, or to be planned, by the individual countries concerned. It seems clear that both the target groups and the means used in any awareness campaigns – not to mention their evaluation – will need to take account of the user configuration specific to each country. Identified data are currently insufficient for proceeding systematically in that vein, however.

¹⁶⁴ The full presentations of the meeting can be found online at:
http://www.saferinternet.org/resources/Barcelona_present.asp

¹⁶⁵ ¹⁶⁵ BDRC, Intermediate evaluation of the Safer Internet Action Plan conducted for the European Commission, Volume one Final report – 31 May 2001

TABLE 1

Country	Population	Online Users figures	Percentage of population
	(in thousands)		
Austria	8 200	2 700	33%
Belgium	10 300	3 200	31%
Denmark	400	2 400	44%
Finland	200	2 235	43%
France	60 000	17 000	28%
Germany	83 000	30 000	36%
Greece	600	1 400	13%
Ireland	4 000	1 300	33%
Italy	7 700	19 250	33%
Luxembourg	450	150	33%
Netherlands	16 000	6 800	43%
Portugal	10 100	3 060	30%
Sweden	8 900	4 600	51%
Spain	40 000	7 900	20%
United Kingdom	59 600	24 000	40%
Total	79 000	126 000	33%

(Sources: ITU, Point-Topic – Nielsen//NetRatings – T3 2002)

TABLE 2

Country	Online users under 17 (%)	Time spent on line per user (hours/month)
Denmark	11.4%	3.3
France	8.2%	3.9
Germany	6.8%	10.9
Spain	6.7%	5.6
UK	11.6%	5.8

(Sources: Net Value – <http://www.netvalue.com>)¹⁶⁶

¹⁶⁶ These figures, from commercial sources, should be seen as indicative. They cover only five countries and are neither detailed enough nor collected sufficiently frequently to constitute a wholly reliable statistic.

b) National characteristics

COUNTRY-SPECIFIC CULTURAL AND SOCIAL FACTORS WHICH IMPACT ON THE INTERNET

Any issue that is tantamount to a moral dilemma is by definition particularly delicate to broach. Mentalities evolve unevenly. Internet pornography as such may be considered variously as desirable, acceptable, a minor nuisance or a major threat. Regional and historical differences and changes are of course substantial.

Furthermore, once the problem has been recognised, the question remains as to what combination of measures could be the most effective to tackle it. In the sphere of criminal activity, there are deeply-held values that cannot be ignored. As a result, while awareness campaigns seem to be one of the most widespread answers to fight against child pornography, they can certainly be neither the sole, nor always even the primary, means used. Here again, legal and social cultures have a strong input in the strategy.

Kuno Sorensen, from Red Barnet Denmark, notes that Denmark has a long-standing tradition of awareness campaigns and a commitment to social education. This national trait also appears to underpin the development of Internet Safety. The vast majority of Danish people have welcomed the introduction of comprehensive awareness projects. The Danish public is now also used to being confronted with strong, direct messages. The challenge of informing children through awareness campaigns seemed unknown in 1997, but it is today a high profile activity in Denmark.

In Finland, a study commissioned by the Ministry of Transport and Communications underlines that legislation alone is not sufficient to prevent harmful content on the Internet: self-regulation and co-operation also need to be promoted, both nationally and internationally.¹⁶⁷ The study also points out that comprehensive solutions are not possible, due to the Internet's vastness, complexity and constant evolution. Prevention of harmful content requires fast actions at both community and societal levels. The study proposes that an open discussion forum and a monitoring group be set up to prevent harmful content on the Internet. The central actors in the field of the Internet in Finland were unanimous in their belief that awareness is the most important and most effective approach to tackle the problem of harmful content.

The strong legal tradition in France has led governments to place considerable emphasis on regulating illicit information through a panoply of legislation. In 1999, Prime Minister Lionel Jospin suggested the need to create a central structure specialised in the fight against crimes connected with new technologies – OCLCTIC, the Central Cybercrime Office (May 2000). An official website for reporting illicit websites (www.Internet-mineurs.gouv.fr) was created in November 2001. It is mainly devoted to housing all useful information on laws and regulations regarding the protection of children in France.

In Greece, a soft approach was recommended, as privacy is important to parents. ChildNet tries to steer a balanced approach between pupils and parents, promoting the positive (e.g. the ChildNet Awards) while responding to the negative.

¹⁶⁷ Mika Rantakokko, see website www.mintc.fi/publications

Although Portugal at present lags behind many of the other Member States regarding Internet access and PC usage, the Government aims to bolster the Information Society in Portugal. Alongside such efforts, current and future users are to be made aware of both the pros and cons of Internet access.

In Sweden, according to a report by Save the Children, there have been relatively few instances of child pornography on the Internet due to Sweden's well-established pro-child legislation and attitude. For example, Swedish children from six secondary and high schools are also involved in the Friendly Internet project whose aim is to cope with Internet risks.

In the UK, a growing number of websites inform Internet users of all ages about potential dangers and how to surf safely, offering advice in designs that reflect the target groups: interactive and colourful websites for children and teenagers, informative websites for parents, teachers and responsible adults.¹⁶⁸ The UK's Home Office Task Force, working on best practice guidelines, believes that the best response is to educate children about the risks associated with Internet.

Despite the differing country realities, Childnet International and Fleishman Hillard research showed that across Europe most adults have similar concerns about safety and the Internet: 'although the team were looking for local manifestations of 'danger' and were sensitive to the country-specific cultural, linguistic and socio-economic factors which impact on the Internet, attitudes did not seem to vary greatly. There appears to be a surprising level of commonality with regards to the appropriate messages and style for communicating safety on the Internet¹⁶⁹.'

EVOLUTION OF NATIONAL PRIORITIES

Changing priorities in a context where a growing number of issues are fighting for limited, if not strictly finite, resources are also a factor that needs to be considered when analysing strategies adopted. Thus:

- the German Government was one of the earliest in Europe to start raising Internet awareness. Its ongoing efforts have resulted in the EC recently taking up a German initiative to fight racist and xenophobic digital content, by informing schools, teachers and educational institutions to be aware of their responsibilities towards the young. It seems that in Germany, racist content is nowadays a priority concern.
- in the Netherlands, via the 'digital research' group, the Dutch police office KLPD is now investigating the form and complexity of illegal Internet gambling. Once the
- study is finished, the government will consider whether and how illegal gambling on the Internet should be tackled.

These two examples serve to illustrate how 'child pornography on the Internet' may run the risk of being sidelined among other emerging Internet-related concerns.

¹⁶⁸ Contribution from Nick Morgan, Learning and Teaching Scotland

¹⁶⁹ Safe use of the Internet, Promoting safe use of the Internet, How to communicate messages about Safe use of the Internet to parents, teachers and children across Europe, Childnet International, Fleishman Hillard, December 1999

9.2.2.2 Assessment Of The Effectiveness Of Preventive Measures – Activity 2

The general goal of all preventive measures related to child pornography on the Internet, including awareness and educational initiatives, is to contribute to the reduction of the overall level of pornographic material circulating on the Internet. However, given the lack of consistent and ongoing monitoring at present, it is not possible to determine the degree to which awareness and educational initiatives in fact contribute to this objective.

The basic assumption therefore has to be that the greater and more complete the combination of the four effectiveness indicators – multiplicity of actors involved, multiplicity of means used, coverage/outreach and sustainability of projects – the higher the numbers of young users online effectively reached (Annex 4).

This notwithstanding, and given the global and borderless architecture of the Internet, effective preventive measures will surely be those that can be best adapted to the specific nature of the Internet, thereby maximising potential outreach to children and their families.

9.2.2.2.1 Multiplicity of actors involved

As noted previously, assuming that it is extremely difficult for an individual organisation or for the government alone to be able to reach a broad target audience, it was of major importance to identify other organisations and companies involved with issues related to the safety of children in the Internet. A mix of actors provides an unrivalled opportunity to reach a broader public.

In almost all countries, more than one actor has been identified, but in very few are there cross-sectoral campaigns involving different actors (government, NGOs, Internet providers, education authorities, law enforcement agencies and European partners)¹⁷⁰. In addition, no country seems to have an effective mechanism in place for the co-ordination of these actors.

However, through European projects, a first phase of identification of multiplier organisations has been completed, and this will contribute to the future implementation of the eSafe programme. For example, the Infonet project (Information on Safer Internet for Italian and Spanish users) has identified a list of multiplier organisations and obtained the support of different institutions, public and private, in order to get them involved in the efforts to make society aware of the need for protecting children against harmful content on the Internet, such as pornography. These institutions could also help in efforts to empower parents and teachers in the protection of children by informing them about tools available for filtering and blocking inappropriate content on the Internet.

Additionally, the SUI project has contacted content providers in various countries to raise their awareness for a safer use of Internet. Providers have been informed of the opinions, needs and hopes of schools, teachers, pupils and their parents¹⁷¹.

¹⁷⁰ Belgium, France, Italy, Netherlands and the UK

¹⁷¹ Final Report to the European Commission SUI November 2001

9.2.2.2.2 Multiplicity of means used

It is assumed that the more means of communication available, the broader the public reached will be.

a) Materials prepared

In order to conduct Activity 2 – effectiveness evaluation – five different groups of means were selected: websites, printed leaflets and brochures, TV campaigns, newspapers and radio.

The phase concerning the development and the adaptation of existing materials and technical solutions is now nearing completion. Much creativity has been devoted to this effort. With the high input of European projects, materials have been selected and successful awareness-raising techniques are or will be translated, adapted and prepared for every country and more generalised use. This constitutes a set of preparatory actions to provide European schoolteachers, and future websites, with effective means for safe Internet use by children.

As a first conclusion, every country – either through a governmental or a non-governmental initiative – has set up a website, although they differ considerably in nature: from a families' online website in France with '*Familles en ligne*', to a website created by a platform of different actors such as Surfopsafe in the Netherlands and one 'for kids by kids online' as in Ireland.

Virtually every country is also using printed leaflets, brochures and guides in order to disseminate information about safer use of the Internet.

In contrast, it appears that only seven countries¹⁷² are using TV campaigns to convey awareness and education initiatives; radio and newspapers are sometimes involved in awareness campaigns but their use could be greatly improved

Some European projects, such as Educaunet, Dot.Safe, Infonet, SIFKaL and SUI, have produced and published integrated packages of tools and media to help adults and teachers implement the education process. Generally, these packages have been tailored to specific groups of children and youngsters (for example 8–11 years, 12–15 years, and 16–18 years); or to other target groups. Under the Infonet project, two versions of each kind of information material have been prepared: one targeting end users (parents, teachers and students), and one with more technical details aimed at ISPs, content providers and Internet IT developers.

Finally, it can be noted that these European projects are creating websites 'with no frontiers'. Zap is a good illustration of this trend: it is a multilingual website for children aged 8–14. Launched in January 2003, it offers tips on 'netiquette' and safe surfing, and is also a place where children and teenagers can learn more about school-related topics and gain Internet skills. The Zap site brings together European Schoolnet and seven other partners (IINDIRE, FCR, eLinq, Birmingham City Council, the Danish Ministry of Education, the Portuguese Ministry of Education and ECSITE).

As far as the appropriateness of the choice of materials prepared in the context of awareness and education initiatives is concerned, however, the European Parliament has already expressed a word of caution, declaring in 2002 that 'the cost-effectiveness to ensure that a large-scale impact of awareness and education

¹⁷² Belgium, Denmark, Greece, Italy, Netherlands, Spain, UK

initiatives was achieved is important¹⁷³. It felt that the intermediate evaluation of the action plan of 2001, presented by the European Commission, revealed that while the Commission had funded a total of 9 awareness projects, specific recommendations on cost-effectiveness were not taken into account. Furthermore, the European Parliament pointed out 'that traditional information packages are too costly; that new media should be used, and that it is essential to distribute information through industry, for example, by informing journalists of relevant magazines and distributing CD-ROMs with magazines. Despite this, projects such as the SUI projects resulted in the distribution of 60,000 copies of a brochure on safer Internet use to teachers, instead of distributing CD-ROMs to schools, which would have been cheaper and made further distribution easier'¹⁷⁴.

b) Nature of the messages delivered

Many actors in the field believe that solutions to the problems should be provided at the same time as information is delivered to parents and teachers. Current updated information about filtering and rating solutions available is vital to complement the awareness messages. Further, messages given to the public should never have an alarmist tone and should not be limited to the negative aspects of the Internet. The education message should contain a critical approach of the risks linked to the use of the Internet. The aims are to help children to develop an autonomous, responsible attitude in their use of the Internet. Conceived in this way, this approach is a necessary complement to existing filters, security and classification tools, which can never guarantee total protection.

In this framework, Childnet International, in co-operation with Fleishman Hillard, undertook a study on how best to communicate safety messages about the Internet to parents, teachers and children¹⁷⁵. The main findings were the following:

- parents have real concerns about the dangers to children using the Internet and are looking for authoritative, reliable and credible advice that will help them ensure that children's/pupil's experience on the Internet is positive and safe;
- parents needs advice as to filtering software;
- many parents stressed that they needed an 'idiot-proof' guide to the dangers and steps to help their children avoid the dangers of the Internet;
- a full Internet Safety programme needs to have three essential elements: protecting children from harmful sites, directing children towards the positive, and developing 'net literacy' among children so that they are aware of the dangers;
- children's ability to use the Internet will be an increasingly essential skill.

¹⁷³ Committee on citizens' freedoms and Rights, Justice and Home Affairs, provisional 2002/0071 (COD) Rev, 6 November 2002 on the Proposal for a European Parliament and Council Decision amending Decision N°276/1999/EC adopting a multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global network (COM (2002) 152 – CS – 0141/2002 – 2002/0071 (COD))

¹⁷⁴ *ibid.*

¹⁷⁵ Safe use of the Internet – Awareness programme, How to communicate messages about safe use of the Internet to parents, teachers and children across Europe, December 1999, See the website: www.netaware.org,

9.2.2.2.3 Coverage and outreach

It is assumed that the greater the dissemination, the broader the public reached will be.

Participation in conferences and seminars has been cited in the majority of the countries. Various opportunities to disseminate knowledge have been exploited, including presentations and workshops at teachers' conferences, parents meetings, and articles for the media. Dissemination is rarely at national level, however¹⁷⁶. Visits to schools have been undertaken to organise activities, conduct pilot projects, and/or engage with teachers and school managers, but again generally as one-off regional or local projects. Through the European projects, after a relatively large-scale pilot testing, plans have been developed to target teachers and other audiences. In this field, we are still at the phase of preliminary dissemination with limited and partial actions. While the foundations for large-scale actions exist in some countries¹⁷⁷, the campaigns have yet to be launched.

Finally, more co-ordination between projects and actors is needed. This is still difficult to establish in many countries, as organisations and industries do not share the same objectives.

9.2.2.2.4 Sustainability of the action

Results achieved also need to be long lasting or permanent, and the research therefore tried to ascertain whether the achievements to date would survive the end of the Action. It is clearly desirable for projects to have a sustained impact after funding has ceased.

Some countries have established special permanent structures¹⁷⁸. For example, in Germany, the Advisory Council for the Internet and the New Media acts as an informal forum for discussion, and in the UK, the Government has established a Task Force on Child Protection on the Internet. Italy has created a National Observatory to monitor paedophile data, promote informative campaigns and a telephone helpline. The French government envisages, for the end of 2003, the creation of an Internet Higher Council in conjunction with 'civil society of Internet users' and experts.

Among other examples are the Foundation Safer Internet in the Netherlands and the Internet Watch Foundation in the UK, which help adults and children when they come across illegal and harmful content. While these foundations work closely with the Internet service providers and police forces, they are also involved in awareness campaigns and education initiatives.

Finally, the European Commission project SIFKaL (Safer Internet for Knowing and Living) has created a 'permanent observatory' for Safer Internet (OFSI), for the dissemination of information, experiences, ideas, documents, links and actions.

All these permanent structures are tasked with helping to organise public awareness campaigns that can be undertaken by industry, education authorities or

¹⁷⁶ Denmark, Netherlands, Sweden and UK

¹⁷⁷ Austria, Belgium, Finland, France, Germany and Ireland

¹⁷⁸ Austria, Belgium, France, Germany, Ireland, Italy, Netherlands and UK

law enforcement agencies. A permanent strategy can be built focusing on on-going information and education programmes directed at consumers or users.

As a general rule, on-going training programmes in schools concerning a safer use of the Internet have not been set up. Additionally, the question of child pornography does not figure prominently, if at all, in whatever training exists. For example, a respondent from the UK underlines that 'education authorities run internal training sessions for their staff in many parts of the UK, but it is likely that child pornography would only be mentioned in passing. The content and coverage of those sessions is mixed and many staff will not have attended one. Updating sessions for staff seem to be rare'.

It is important that 'awareness sites' have high visibility and accessibility in major search engines. These sites need to be cited systematically in awareness campaigns, or where necessary set up as part of the campaign. It is also crucial that individual agreements with various portals are reached. All the material and the results of the actions taken for the awareness campaign should be constantly communicated and presented to the multiplier organisations involved. This does not seem to be the case at present.

As regards the impact of European projects from a sustainability standpoint, the participants at the 'Protecting and educating children in the information society: lessons from European projects' conference, Barcelona, 15 October 2002, noted that in many cases their activity was unlikely to have started without IAP funding. To this extent, the Action Plan has had a direct and beneficial impact, but reductions in funding – e.g. because of new priorities – seemed likely to constitute a potential problem in the very near future.

9.2.3 Concluding Remarks

At this stage of the research and on the basis of data gleaned to date, it would be pretentious to set out fully-fledged conclusions and recommendations. A number of short final comments may nonetheless be in order, as possible pointers for further study and future action.

The review of awareness and educational initiatives has brought to light the variety of approaches to the problem of illegal and harmful use of the Internet in EU Member States. This heterogeneity of the measures is not surprising, given in particular the newness of the issue, cultural differences and variations in the development of Internet from country to country. Furthermore, six years may be a rather short period over which to apply European legislation and evaluate compliance with it.

Despite this diversity, there seem to be a number of common realities. One is that a very clear felt-need exists for visible (and easily-accessible), constructive and practical information regarding safety on the Internet. A second is that, while a number of efforts have been made to meet this demand, they tend not to be co-ordinated and in no way do they reap the benefits that would come from combining the forces of the various kinds of actors involved. A third would surely be the need to ensure the sustainability of projects launched – including repetition of awareness and educational initiatives at appropriate intervals.

For the moment, self-regulation seems the best way to promote good practice, but it needs to be backed up by government measures. An integrated system of self-

regulation and end user autonomy should not be synonymous with the disengagement of the authorities of Member States and Internet providers. On the contrary, it requires a sense of responsibility, strong co-ordination of the many different players involved (as noted above, this is still in its infancy), and continuous (re-)evaluation of awareness and educational initiatives.

Indeed, no single approach, relying on one form or one set of actors, can provide a solution in the constantly changing Internet environment. The effectiveness of self-regulation depends greatly on full collaboration and commitment among all actors. Governments should through education and public information 'share a responsibility to communicate Internet Safety to citizens', to raise awareness among users of self-regulatory mechanisms such as the means to filter and block content and to communicate complaints about Internet content through hotlines, and to establish permanent educational programmes for pupils. Awareness and educational initiatives may be directed specifically at teachers and the education sector. Here, the Bertelsman Foundation recommendation in 1999 has lost none of its validity: schools should provide the necessary skills for children to understand the benefits and limitations of online information and to encourage greater self-control over problematic Internet content. Other initiatives will have a broader focus aimed at the general public (parents and children). In both cases, however, they should avoid an alarmist thrust and should develop a positive approach to the Internet and its possibilities. Children should clearly be directly involved in the development and, as far as possible, the dissemination of child-focused messages.

Finally we can note that in the eSafe Directions for 2003-2004 Discussion Paper, the European Union considers that effective safer Internet awareness raising is most cost-effective when organised on a national basis, but co-ordinated at European level. Therefore it would seem to be a priority to establish an awareness node in all Member States and in candidate countries.

10.

FINDINGS OF THE STUDY RELATED TO AREA OF INTERVENTION D (TECHNOLOGICAL MEASURES) BY UNISYS BELGIUM

10.1 INTRODUCTION

The present report constitutes the Unisys' contribution to the research project entitled 'Child pornography on the Internet. Evaluating Preventive measures in order to improve their effectiveness in the EU Member States awarded by the European Commission in December 2001 (contract 01/097/C signed on 12 December 2001) in the frame of the Daphne Programme.

More specifically, this report constitutes the Task 1 and 2 of Unisys' area of intervention, namely area of intervention D: technological interventions.

The objective of the first part of this report is to make an inventory of the existing technological measures and devices that can be used today in order to help protect children against exposure to pornographic material and contact with pornographers and paedophiles. A number of measures and technological possibilities aimed at reducing the anonymity of Internet users (and abusers) have also been presented.

The second part goes one step further: it aims at evaluating the effectiveness of the technological preventive measures and devices available today.

Background

The production and spreading of illegal Pornography has risen precipitously in the last years. In the past the exchange was limited to physical passing on of pictures and film material. With the invention of new technologies, and especially the popularisation of the Internet, the methods and the amount of spread material have changed too.

The Internet is an amazing invention that shrinks distances and enables a considerable amount of information and knowledge to circulate at an astonishingly high speed. Unfortunately, the spreading of undesirable and even harmful material, such as incitement to drugs abuse, violence, racial hatred, and sex, for instance, is facilitated by the same token. And part of the information spread through the Internet, like child pornography, is illegal in most countries.

Besides, manufacturers provide new technological means of creating and spreading illegal pornographic material. For instance, the digital camera makes it very easy to produce and spread amateur pictures. It is even possible to make a digital video by using a sophisticated version of this device. This digital camera is very often used to create pornographic material, including child pornography, which is then spread through the Internet.

Every year thousands of children are being killed emotionally or even physically by the production of child pornography.

Given the trans-national dimension of child pornography on the Internet, the EU believes that an effective prevention of this criminal phenomenon needs a European common approach, which will allow conducting most activities jointly in all EU Member States.

Purpose and scope

The purpose of the present document is to report on the existing technological interventions that can be set up in order to prevent or reduce the spreading of child pornography on the Internet.

The scope of the present document is to map and describe the existing technological devices used for the prevention of child pornography on the Internet, in the European Union and beyond. The differences among the different devices will be highlighted.

Structure of the document

The present document starts with an introductory section that briefly describes the background and purpose of the project. It then focuses more specifically on the scope of the present document, presents its structure, the method of data collection and ends with a list of acronyms. The document is then structured in four more sections and one annex.

Section 2 describes how the various Internet channels are used by child pornographers and paedophiles.

Section 3 makes an inventory of the different protective technical devices available today to exert a certain degree of control over the material that is spread or accessed via the Internet.

Section 4 describes the techniques and tools available to trace Internet abusers, together with their limitations.

Finally, Section 5 presents the conclusion of this study.

A technical overview of the Internet world is presented in annex. The annex has been written keeping in mind that the reader might not be an IT literate. The purpose is to allow every single reader of this report to grasp the size of the problem at hand and understand the functioning of Internet in its several different aspects. By the same token it will also permit to understand the functioning of the existing technical devices that can be installed to limit the visibility and spreading of unwanted material, and of the traceability techniques that can be implemented to track down Internet abusers.

Method for data collection

The investigated data in the report was collected through:

- the Internet;
- information received from contacts with other organizations fighting against child pornography on the Internet;
- information received from manufacturers of technological devices;
- magazines that have published information about the prevention of child pornography.

10.2 LIST OF ACRONYMS

ADSL	Asynchronous Digital Subscriber Line
AOL	America On Line
ARPANet	Advanced Research Projects Agency Network
BKA	Bundeskriminalamt (Germany)
CA	Certification Authority
CFV	Call for Votes
CLI	Calling Line Identification
DNS	Domain Name Server
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
mIRC	Mardam-Bey's Internet Relay Chat
NAT	Network Address Translation
NNTP	Network News Transfer Protocol
NSFNet	National Science Foundation Network
PICS	Platform for Internet Content Selection
POP3	Post Office Protocol
RDF	Resource Description Framework
RFD	Request for Discussion
RSAC	Recreational Software Advisory Council
RSACi	Recreational Software Advisory Council Internet
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
UUCP	Unix-To-Unix Copy Protocol
W3C	World Wide Web Consortium
WWW	World Wide Web
XML	eXtensible Markup Language

10.3 CHILD PORNOGRAPHY ON THE INTERNET

The Internet is a wonderful medium for spreading information about all kinds of topics. People can communicate and discuss by e-mail, IRC, newsgroups. They can find and provide information. The Internet is really an amazing invention.

But the Internet also has its dark side. Hate mails, racist speeches, pornographic material, bomb and drug formulas, and other sensitive and inappropriate information is being freely available along with everything else.

Not all areas of the Internet medium are equally dangerous. Some are quite safe and other places are potentially dangerous.

This chapter explains how child pornography information is presented on the Internet by discussing the different mediums available via the Net.

A basic technical description of the functioning of Internet in its different aspects is provided in annex.

World Wide Web

The websites, which provide child pornography material can be divided into three groups:

- **Free websites.** These are usually published by paedophiles. They want to share their interests with other likeminded people by providing a complete website presenting the material they gathered. Some of these web sites promote paedophilia as a lifestyle. These sites help those who prey on children to rationalize their feelings. Sometimes they also provide information on how to find child victims and child pornography in other parts of the Internet.
- **Fee-charged websites.** These are particularly published by child porn traders on the web. The first page of the site is usually free of charge and presents an overview of the complete site in order to seduce paedophiles. If someone wants to see more information, a fee is charged. After paying the fee, a password to enter the complete site is sent by e-mail.
- **Popup windows.** These are the advertising windows that are displayed without asking for, when visiting some 'innocent' web sites. These popup windows are used to advertise the fee-charged websites published by child porn traders.

E-mail

Child porn traders and paedophiles use the e-mail service to exchange information such as pictures, stories, links, videos etc to likeminded people.

But child porn traders also send this material to people they do not know, hoping they would get interested in buying after reading the e-mail. They just choose the people's e-mail addresses from the lists of addresses available on websites for instance. Here are two examples of websites that provide lists of e-mail addresses:

- <http://www.bigfoot.com>
- <http://www.four11.com>

Anonymity

Although e-mails are always accompanied by an e-mail header, which contains information such as the address of the sender and the machine from which the e-mail is sent, paedophiles believe it is possible to remain anonymous.

They try to do this by using a fake e-mail address. This is possible simply by changing the 'Sender' and the 'Return-to' fields to something different. This is easy since normally these fields are not checked by the mail server when sending an e-mail, they are only checked when an e-mail is being received.

It is also possible to send e-mails via 'Anonymous Remailers'. Anonymous remailers receive the e-mail messages and they re-send them, without revealing the identity information of the sender. The 'sender-info' is stored in a table so as to identify the sender when there is a response to the e-mail (See Figure 1). Thus when the mail is sent, the recipient cannot identify the sender anymore.

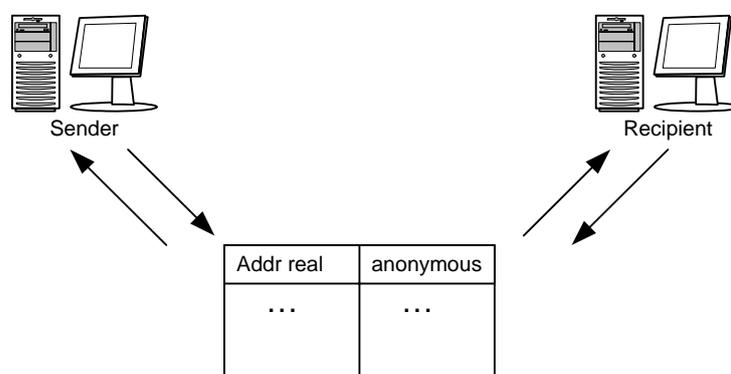


Figure 1 – Anonymous Remailing system

Another method used to remain anonymous is to have free e-mail accounts available on the Internet, such as Hotmail and Yahoo. People simply use fake identity information when registering to these free mail services.

Most people believe they can use anonymous remailers and other techniques to remain anonymous by hiding their IP address and make their movements on the Internet untraceable, but actually anonymity is not always complete.

As a matter of fact, even the anonymous remailing systems keep logs. Remailers can see which IP address and which ISP a person used not only when first opening the account, but also each time this person uses his anonymous account. So in theory, everything is traceable back to the IP address. The anonymous remailing system provider can trace back to the IP address a person who usually logs onto their server, and that number allows tracing back that person's machine. Of course this is only possible as long as logs are available. But logs are not kept forever, typically they are kept until the service provider might need them, then they are deleted.

E-mail address lists

People spreading child pornography material get addresses from several sources. The addresses are stored in databases, and are often sold to other perpetrators.

Once someone's address gets into such a database, he can be bombarded with lots of unwanted e-mail messages.

Table 1 presents some of the most common sources of e-mail address lists and how these addresses are collected.

Sources	Means of collection	How the addresses are collected
The recipient himself	The recipient responds to a message	A person receives a mail, which includes an e-mail address and he is invited to respond to that address if he does not want to receive these mails anymore. If the receiver responds to these messages, he generally confirms that the address was correct. The sender may put the address on a confirmed 'known addresses' list instead of removing it.
Newsgroups	Robot	Software tools called 'robots' search through the newsgroups and collect e-mail addresses from the messages.
Websites	Robot	Robots search through websites looking for e-mail addresses. If the author includes an e-mail address link, the robot may find it.
Online Services (MSN, AOL, CompuServe, etc.)	Robot, Members	Robots scan various chat rooms and collect e-mail addresses. They can also scan member directories, if available. Sometimes the e-mail senders join special services to collect addresses.
Online Software Registration	Purchase	Online registration forms often include options for adding or removing the your name from corporate mailing lists. Sometimes one has to specifically indicate that he does not want his address on the list; otherwise they automatically add him to it.
Electronic News Subscriptions (E-zines)	Purchase	Online news services like PointCast often give the option to receive advertisements from other companies that purchase the lists.

Table 1 - Sources of e-mail address lists and method of collection

Newsgroups

Newsgroups are very efficient communication channels. Interesting information on special topics can be found using newsgroups. Another advantage is that users can remain anonymous.

The content of this section is based on information received via email from the organisation www.houseofthedead.org.

The messages posted on newsgroups also contain a header, like in e-mails, with information about the user and the machine from which the message was posted. And like they do with e-mail headers, pornographers try to forge this information too.

Thus this anonymity is also a large disadvantage of newsgroups. It facilitates the spreading of child pornography. People like paedophiles can easily and anonymously exchange information about child pornography through newsgroups.

The following newsgroups are examples of newsgroups about child pornography¹⁷⁹:

- alt.binaries.pictures.teen.nonude;
- alt.binaries.pictures.boys;
- alt.binaries.pictures.erotica.children;
- alt.binaries.pictures.erotica.pre-teen;
- alt.binaries.pictures.erotica.early-teen;
- alt.binaries.pictures.erotica.11-series;
- alt.binaries.pictures.youth-and-beauty;
- alt.binaries.adolescents;
- alt.pictures.erotica.mclt;
- alt.binaries.pictures.bc-series.

These newsgroups come and go, changing servers and names occasionally. Some Internet Providers do block some of these groups, but it is almost impossible to block them all.

Each day hundreds of pictures of child pornography are being posted in groups. The members of the groups post these pictures without fear of being caught. If the group eventually gets caught, the operators of the group just start another one.

These groups have been around for years, in some cases, and members come and go. They may leave for extended periods, and then return much later. Groups generally have a high turnover rate, but usually there are several key people in any given group. These members

are most likely somewhat knowledgeable in computer technology, and sometimes retain a certain hold on the group with the power to manipulate not only the contents of the newsgroup, but also its members.

Chat services

Chat services are also an interesting medium for child porn traders and paedophiles for spreading material. Especially IRC is commonly used by child pornographers either to share their views and material, or to lure children.

Most of the people that are found dealing child pornography in specialised chat rooms are beginners. They are new and have heard from people who are used to it

¹⁷⁹ This list shows only SOME of the actually available newsgroups which have been known to contain content deemed to be child pornography according to US laws, 18 U.S.C. § 2256 (<http://www.adultweblaw.com/laws/childporn.htm>). The list was provided by www.houseofthedeath.org.

that chatting is a good place to start. These people are usually unskilled in computers and are not connected to any other bigger child porn rings. They are mostly chatting to establish some sort of relationship with other likeminded people, because these people are eager to share their web links, FTP servers, and other resources with those they think are of like mind.

Paedophiles also use chat rooms for other purposes. They infiltrate children or teens chat rooms especially to lure children into conversations about their sexual desires. The paedophile then attempts to arrange deeper contacts with the children with a view of establishing and developing a sexual relationship with them in the 'real world'. Such relationships can then be pursued through other media such as e-mail and mobile telephones. Usually these paedophiles pretend to be of the same age as the children they want to meet and therefore access teen's chat rooms.

File transfer via FTP

FTP¹⁸⁰ is an efficient service to transfer files of all formats over the Internet from one computer to another. Files can be transferred between computers running on different platforms, such as transferring files from a UNIX computer to a computer running Windows. FTP services thus facilitate the spreading of child pornography material on the Internet too.

Anonymous FTP allows users to copy files from remote computers without having an account. These files are publicly accessible in this way. There are lots of servers that provide anonymous FTP access, where files are stored and made available for others to copy freely. Figure 2 shows an example of a connection window of a piece of software (LeechFTP in this case) that allows using FTP anonymously.

When transferring publicly accessible files, one only needs to use the word 'anonymous' for the login name when connecting. To be polite to the administrators, the user normally provides an e-mail address as password, but it is not mandatory.

¹⁸⁰ The information contained in this section is based on the CERT Coordination Center, Anonymous FTP Abuses, http://www.cert.org/tech_tips/anonymous_ftp_abuses.html.

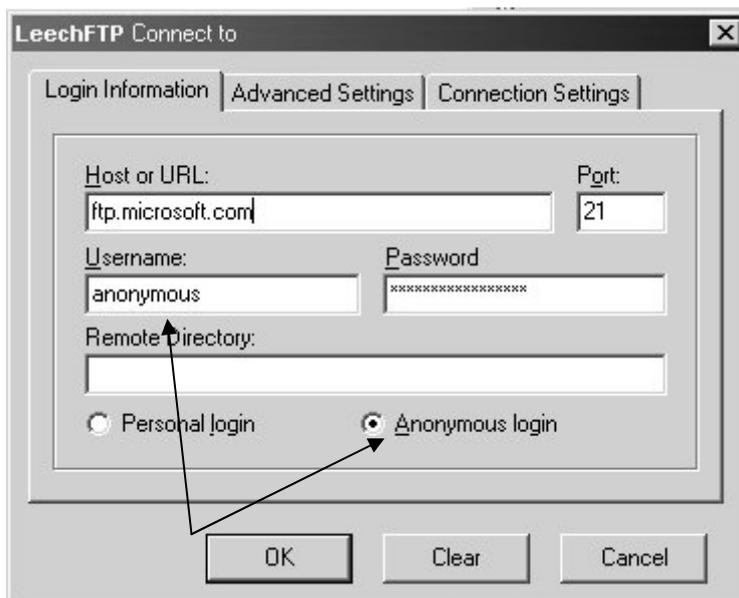


Figure 2 – Connection window of the LeechFTP client

Peer-to-peer networking over the Internet

Technologies such as Napster and Gnutella have recently been popularised as a means of enabling people to exchange music or other types of files across the Internet.¹⁸¹ They allow anyone with an Internet connection to become both a server and client thus allowing people across the world to connect directly to each other's machines without having to use a third.

Child pornographers are already using these technologies to communicate directly with each other. They use these Internet file-sharing programs, as they are also called, to share their indecent and illegal material such as child porn videos and pictures. When this technology is used, the possibility of detection is even more reduced.

Sometimes people looking for ordinary music or other 'innocent' files are exposed to child pornographic files. This is because the peer-to-peer file-sharing software allows entering search queries. And sometimes these queries contain child pornographic files in the result. These files do not reveal the real topic in their title, so that the user opens the file without knowing what it is about.

And what is worse is that the most popular protective technological devices do not block access to the indecent material obtained through file-sharing programs. One can install programs that block child pornographic pictures on the Web, but not all of these programs are capable of blocking the material sent through a peer-to-peer network.

Examples of these peer-to-peer file-sharing programs are BearShare, Aimster, LimeWire, Music City, Morpheus and KaZaA.

¹⁸¹ John Carr noted this in his paper on Child Pornography for ECPAT (www.ecpat.net) http://www.focalpointngo.org/yokohama/PDF/en/Yokohama/Background_reading/Theme_papers/Theme%20paper%20Child%20Pornography.pdf

10.4. PROTECTIVE TECHNICAL DEVICES

In response to the easy, fast and uncontrolled spreading of unwanted material on the Internet, people can make use of several technological devices to protect themselves, and their family. The purpose of this study is to map the different technological devices that can be used as a preventive measure against child pornography on the Internet. This section will be entirely devoted to that very topic.

The most commonly known devices are filters and rating systems, but other techniques such as image scanning are also available. This section will present those different devices explain their modes of functioning together with the different possible implementation approaches.

Platform for Internet Content Selection or PICS™

PICS is a cross-industry working group whose aim is to facilitate the development of technologies that would give Internet users a certain control over the kind of material they have access to.

The PICS standard is a set of technical standards developed by the organization W3C that enables site constructors to distribute a description of their site electronically. This description, called 'label' is in fact metadata, which is associated to the site content.

PICS labels are then used by protective devices, such as filters or rating systems, to decide whether or not a content found on the Internet may be displayed (or downloaded) on the user's machine¹⁸².

How PICS™ works

PICS is an open standard for the development of rating systems and is used in two different ways, namely self-rating or third-party rating.

Publishers of a web site can perform their own evaluation and labelling of their sites. The Recreational Software Advisory Council (RSAC) and SafeSurf are two organisations that use the PICS standards and distribute labels that permit developers to rate their own web sites according to specified criteria.

The Recreational Software Advisory Council (RSAC) adapted its computer-game rating system to the Internet. Each RSACi (The 'i' stands for 'Internet') label has four numbers, indicating levels of violence, nudity, sex and potentially offensive language.

SafeSurf, developed a vocabulary with a nine-degrees scale. Their system contains the categories 'Age Range', 'Nudity', 'Violence', 'Profanity', 'Sex, Violence' and Profanity', 'Intolerance', 'Glorifying Drug Use', 'Other Adult Themes', and 'Gambling', with nine distinctive degrees for each category.

The web site developer who wants to label his site connects to a web server of one of those two organisations and fills in an online questionnaire that describes the site to be labelled. Then the developer receives a textual label in a particular format that the developer adds to its site. When a labelled site is loaded, these labels are

¹⁸² For more information about PICS see: <http://www.w3.org/PICS/> and EFA, Content Rating and Filtering, <http://www.efa.org.au/Issues/Censor/cens2.html>.

loaded too, allowing specific filtering systems, and browsers, to determine whether or not the site may be accessed. Certain search engines also make use of PICS labels in their selection criteria.

Not all web sites publishers are keen on labelling their sites. They most probably will not do it if their web sites contain illegal material. To cope with this problem, groups of people offer external and independent labelling services using the PICS standard.

Some manufacturers of rating systems have also a group of people who scan the Internet and label sites, using either PICS labels or their own.

Because labelling can be performed by different parties, the same content may receive different labels from different sources.

General format of a PICS label:

A PICS label generally consists of a service identifier, label options, and ratings. The service identifier is the URL chosen by the rating service as its unique identifier. Label options give additional properties of the document being rated as well as properties of the rating itself, such as the time the document was rated. The rating itself is a set of attribute-value pairs that describe a document along one or more dimensions. One or more labels may be distributed together as a list.

The general form for a label list is:

```
(PICS-1.1
  <service url> [option...]
  labels [option...] ratings (<category> <value> ...)
    [option...] ratings (<category> <value> ...)
    ...
  <service url> [option...]
  labels [option...] ratings (<category> <value> ...)
    [option...] ratings (<category> <value> ...)
    ...
  ...)
```

Distributing a label

According to PICS, there exist several ways to distribute a label along with Internet documents. Three methods are explained hereafter

- If allowed by the HTTP server, PICS recommends inserting an extra header in the HTTP header stream that precedes the content of documents that are sent to web browsers. The server can send these headers even if the browser has not specifically requested them. The correct format is to include the two headers, Protocol and PICS-Label:

```
HTTP/1.0 200 OK
Date: Thu, 30 Jun 1995 17:51:47 GMT
Last-modified: Thursday, 29-Jun-95 17:51:47 GMT
```

```
Protocol: {PICS-1.1 {headers PICS-Label}}
PICS-Label:
(PICS-1.1 'http://www.gcf.org/v2.5' labels
on '1994.11.05T08:15-0500'
exp '1995.12.31T23:59-0000'
for 'http://www.greatdocs.com/foo.html'
by 'George Sanderson, Jr.'
ratings (suds 0.5 density 0 color/hue 1))
Content-type: text/html
...contents of foo.html...
```

- The next best method according to PICS is to run a label bureau at a specific location on the used server, distributing labels only for documents on that server. This server creates a label for the requested URL at runtime.
- If neither of these methods is available, a simpler but more limited method is to embed labels in HTML documents using a META tag. This method only enables to send labels with HTML documents, but not with images, videos or anything else. This method also requires that the labels be inserted into every page of the web site, which represents a lot of work and is time consuming. The following example shows how to embed a PICS label in an HTML document:

```
<head>
<META http-equiv='PICS-Label' content='
(PICS-1.1 'http://www.gcf.org/v2.5'
labels on '1994.11.05T08:15-0500'
until '1995.12.31T23:59-0000'
for 'http://w3.org/PICS/Overview.html'
ratings (suds 0.5 density 0 color/hue 1))
'>
</head>
```

...contents of document here...

One remark: it is tolerated to put more than one META tag in an HTML document. This makes it possible to provide labels according to several services.

The future of PICS: the Resource Description Framework (RDF)

As the syntax of a PICS label is very compact and does not use any of the subsequent Web technology such as XML and XSL, a separate W3C working group is developing a new label format, called Resource Description Framework (RDF). Resource Description Framework labels will be based on XML and will be able to express everything PICS labels can express plus extra possibilities. The added features of RDF Labels will permit even more refined categorisations than what exists now with PICS

Filters

Internet content filters¹⁸³ are tools that enable the users of the Internet to control the information they receive. Filtering can take place at several locations, on a user's PC, on a server within an organization, as a service provided by an ISP, or by means of a third party site.

Filters can be integrated in browsers and search engines. They can also be provided by ISPs. Finally the user can buy and install specific filtering software on his machine.

- **Browsers:** Though not widely known, Internet Explorer and some versions of Netscape Navigator contain a filter. This filter is based on the principle of labels and can be activated by the user according to his needs.
- **Search engines:** Search engines can also contain a filter. This filter is not activated by default but it is easy to do so. AltaVista, for instance, is equipped with a filter.
- **Internet Service Providers:** Some ISPs, for instance AOL in France and in the United Kingdom, offer the service of activating a filter to their subscribers
- **Specific software:** These are programs written by specialized companies. The software is available on CD-rom or may be downloaded from the company web site.

Internet content filters have various functionalities. They can limit on-line activities like chat, e-mail, file downloading, browsing, newsgroups etc. But they can also limit the time spent browsing, and provide reports about on-line activities.

Various types of Internet content filter are available on the market today. They vary in the functionalities they offer, but all have the same goal: to control the information the user, or people under the users' supervision, receives while using the Internet.

Approaches to content filtering

There are two approaches to filtering, namely inclusion filtering, and exclusion filtering.

¹⁸³ The sources of information about filters presented herein are mainly CSIRO, Commonwealth Scientific & Industrial Research Organization, Access Prevention Techniques for Internet Content Filtering, Prepared for the National Office for the Information Economy <http://www.cmis.csiro.au/Reports/filtering.pdf>. Extra information found on Safer Internet.org, <http://www.saferinternet.org/index.asp>, Stanford Computer Science Education - CSE Filtering and Pornography <http://cse.stanford.edu/classes/cs201/projects-98-99/online-pornography/index.html>.

Content filters are based on checking lists of URLs. Third Parties create these lists. They do this by using a web-crawling tool that searches all sites containing words that are deemed inappropriate. Then a team of human beings verifies that the sites found by the web-crawler really contain inappropriate material and not safe and educational information.

The filtering method based on using lists is applied in two different ways:

- **Exclusion filtering:** Exclusion filtering is based on blacklists. Blacklists are lists containing URLs of sites that should not be accessible to anyone using the filter. Blacklists are divided in categories, like for instance, 'Profanity' and 'Drug use'. This enables the user of the filter to select what kind of information he does not want to receive. This type of list filtering is also called 'negative filtering'
- **Inclusion filtering:** Inclusion filtering is based on whitelists. Whitelists are lists of web pages that may be seen. Parents who want to control their children's online activities especially use this method of filtering. It creates a secured environment, which gives Internet user only access to a limited selection of the Internet. Since there are many more 'good' than 'bad' sites, inclusion lists will be longer than exclusion lists. Inclusion filtering is also referred to as 'positive filtering'.

The lists can be stored on a users personal machine or on a server. In the latter possibility the lists are accessed during each surf session and are automatically updated during this session. When a list is stored on a personal machine, the user himself has to do an update from time to time.

When using lists that are stored on a personal machine some providers of lists allow users to customize the lists.

However, having the possibility to do an update of the lists and to edit the lists does not mean that one is also able to see the lists and know which pages are actually blocked. Only a few list providers allow this functionality.

Filtering Methods

The functionalities that filters offer are implemented in different ways. The methods described in the present document are widely used by many filtering vendors. Some are used as a stand-alone method; others are used in conjunction with each other.

1. Filtering based on keyword lists

The method based on keyword lists uses a list of objectionable words, created by the developers of the filter. The list contains single words without context such as 'sex', or 'breasts', for instance.

Filtering systems using keyword blocking can do this by blocking the keyword in the content or the keyword positioned in the URL.

- **Keyword blocking:** A filter using keyword blocking checks each time a page is loaded if the content of the page contains objectionable words from the blacklist. When the filter discovers such a word, two different scenarios can take place. In the first one, the words are replaced by 'xxx', which is called x-ing out. The second one is by blocking the complete page and showing a message indicating that the page has been blocked.

- **URL blocking by keyword:** A filter using URL blocking by keyword checks each time a website is loaded if the URL contains an objectionable word from the blacklist. When the filter discovers such a word the site is blocked and a message of this fact is shown.

Some filters use a new technological method that analyses the language around keywords. This filtering method is called '**Profile filtering**' and examines the characteristics of the received content, rather than checking URLs and keywords on lists. Profile filtering avoids blocking innocuous information such as 'breast cancer' or 'chicken breast recipe'.

2. *Filtering based on rating systems*

An alternative to keyword filtering is filtering based on the labels that describe the web page content. Filtering based on labels are called 'rating systems'.

Rating systems are in fact a series of categories and graduations within those categories. Each category describes the nature of the content such as 'Race', 'Sexual content' or 'Privacy'. Within these categories further specifications are made such as 'Romance; no sex', 'Explicit sexual activity', or somewhere in between.

Publishers of a site can evaluate their own site by using these rating systems. Then they indicate the labels directly on their site. This method of using rating systems is called self-rating.

Third parties make use of a second method for rating systems called third-party rating. These organizations and groups evaluate the web sites of individuals and indicate labels to the content.

Individuals and groups can develop rating systems by defining categories and ratings within those categories. PICS enables anyone to create rating systems.

When loading a labelled site the labels given to the site are loaded too. This way the browser or a specific filtering system checking the labels can determine if the content is appropriate or not for the person loading the site.

Figure 3 illustrates how filtering based on rating systems works:¹⁸⁴

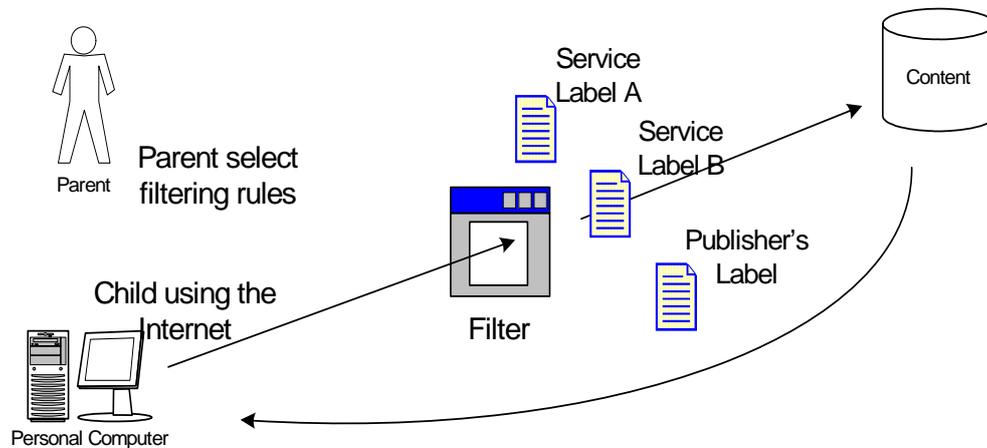


Figure 3 – Filtering based on Rating Systems

In the scenario illustrated in figure 3, a parent controls the activities of his child by selecting specific filtering rules based on rating systems. When his child tries to load Site Y for example, the filter first checks the labels given to the content. Site Y has been given 3 labels. One by the rating service A, one by the rating service B and one given by the publisher of the site himself. Thus, when the browser loads Site Y, the filter checks if the labels given are tolerated according to the rules indicated by the administrator and if the 3 labels pass this check the site is shown. If not, the child receives a message telling that he is not allowed to view this site.

3. Packet filtering

Besides keywords and labels filtering, a third possibility is packet filtering. As explained in a previous section of this document, the content travels through the Internet in packets of information. Each packet has the IP address of where it is going to, as well as the IP address of where it comes from. Packet filtering involves examining the IP address of where the content has come from. If a machine has been identified as spreading illicit content, IP address filtering will block that spreading.

Packet filtering takes place on a router, because routers steer packets through the Internet from source to destination.

4. Filtering based on analysing images

Some filtering products examine the content of images. This is a relatively recent approach and is based on techniques such as the detection of skin tones or on the analysis of the images themselves.

¹⁸⁴ The figure is based on a figure from the article 'Filtering information on the Internet' written by Paul Resnick in 1997 and published in 'Scientific American', <https://www.sciamarchive.com>. The article can be read after a free registration for the archive.

In this approach the image needs to be loaded before it can be analysed. While the image is being loaded, it may be displayed on the user's screen. Therefore this method of filtering is often used in cooperation with URL filtering.

Another solution is to perform the filtering at the ISP level. Then the images can be analysed at the ISP premises before they are displayed on the user's screen.

Other filtering functionalities

In addition to the basic filtering functions some devices provide a number of other protective functionalities.

- **Reporting:** Some filters provide the users with a tool to create the list of web sites that have been visited in a specific period.
- **Time schedules:** Another added functionality is the possibility to create time schedules indicating from when to when the Internet can be accessed. Parents controlling the time their children spend online especially use this too
- **Personal data controlling:** this tool checks the data the user sends. The data is checked for the name, address, credit card number, etc.
- **E-mail:** Some filters can also control the exchange of e-mails. The tool allows sorting the e-mails based on a wide variety of criteria. For example, it is possible to have messages containing the words 'Child pornography' to a special folder. It is also possible to have the message of known senders or on special content categories automatically deleted. Almost all commercial e-mail programs support the use of e-mail filters. A step-by-step guide is usually available in the help file of the program.
- **Newsgroup and IRC controlling:** Some filters can also control the exchange of e-mails, newsgroups and chat sessions. Parents can for example indicate a list of possible addressees and senders
- **Other:** Virus protection, locking of specific software on a computer.

Location of content filtering

Internet content filtering can occur on three locations of the Internet network. It can occur on a user's computer, on the ISP's computer or at a third party location.

5. Filtering on the end user's computer

End users can run filtering software on their own computer. The user's requests are checked against a provided blocking list or white list. The user's request is either allowed or blocked. Figure 4 illustrated the process. Because web sites and pages change frequently, the user must take the initiative to update the list periodically from the supplier of the software.

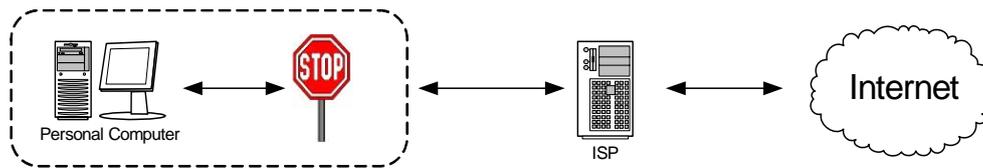


Figure 4 - Content filtering on the User's computer

6. Filtering on the ISP's computer

At the ISP premises, the ISP checks a user's request, by comparing it against a blocking list.

The company that provides the filtering software to the ISP may supply a filter list or filter lists created by third parties. Whatever the arrangement, the ISP's copy of the filter lists needs to be updated at regular intervals, ideally on a daily basis.

Figure 5 illustrates content filtering by the ISP and how a third party regularly updates the ISP's filter list.

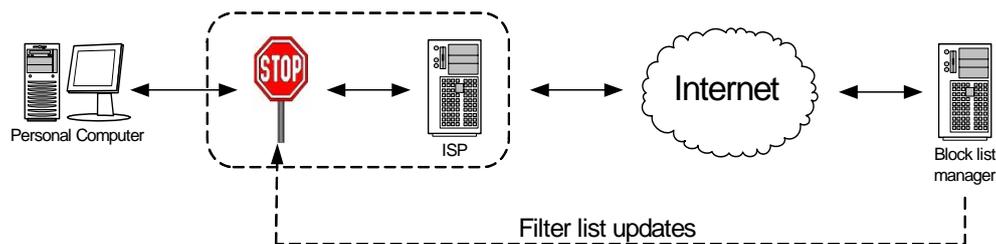


Figure 5 - Content filtering by the ISP and update of ISP's filter list by a third party

ISPs can perform content filtering by using several techniques. The most common technique adopted by ISPs is using a proxy filter. All the clients of the ISP must go through the proxy server in order to access the Internet. Consequently, all ISP clients must configure their software to 'point to' this proxy server to be able to access the services of the Internet.

A proxy server can be selective about what it blocks, and can be configured to block or to permit access to a range of Internet-based services, such as the World Wide Web, newsgroups, FTP sites and chat rooms. Figure 6 illustrates how content filtering by an ISP using a proxy filter works:

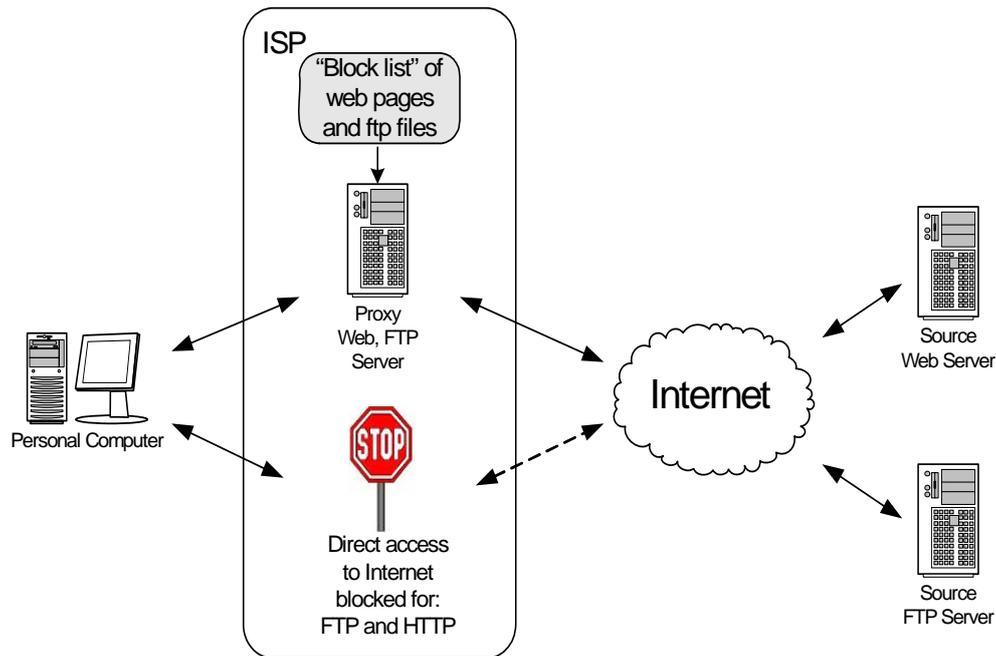


Figure 6 - Content filtering by an ISP using a proxy filter

When a user requests a particular web page or an FTP file, the following process takes place:

- The proxy server checks whether or not the requested URL is on its filter list.
- If the URL is on the filter list, the user is informed that the page or file is unavailable.
- If the URL is not on the filter list, but is currently in the cache of the proxy server (as a result of being requested recently by another user), the requested page or file is sent to the user from the proxy.
- If the requested material is not in the proxy server cache, the ISP issues a request for the material from its source on the Internet.

If proxy filters are used, the users' requests are checked before any content is retrieved.

The content-based filtering approach is different from proxy filtering, in that it checks the content after it has been called from its source and delivered to the ISP.

The requests from the users pass through the ISP to the Internet. The content is retrieved from the source machine, and returned to the ISP. The characteristics of the returned content are extracted by the ISP and compared with the characteristics profile of blocked sites. This is illustrated by figure 7.

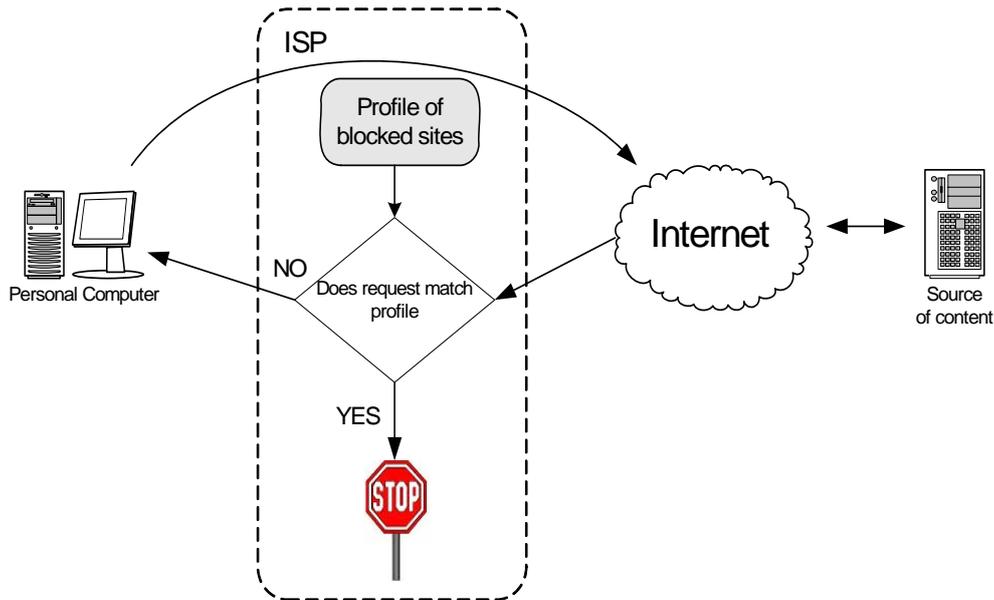


Figure 7 - Content-based filtering by an ISP

Some ISPs provide their clients with both a filtered and an unfiltered service. This may be provided in two ways:

- The ISP provides a different access point to each type of service such as different phone numbers to connect.
- There is a common access method, but an override facility is provided to enable the proxy filter to be bypassed.

7. Filtering by a third party

In this situation, all the user's requests are passed through the ISP directly to a nominated third party, where each request is checked against a filter list.

For this to be effective, the end user's browser must be configured to 'point to' the third party's website for any request. It should not be possible to access the Internet without going through the third party's site. This is illustrated in figure 8.

Various filtering options can be offered, including black list and white list filtering.

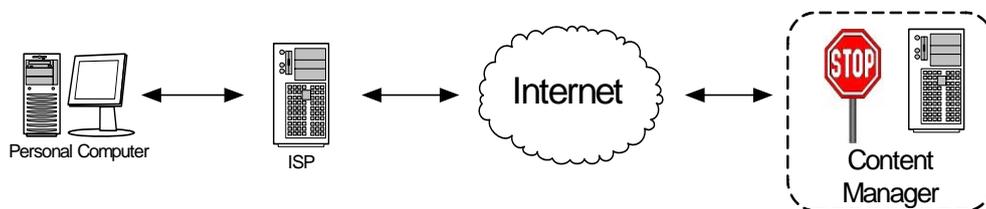


Figure 8 - Content filtering by a third party

A variation of this arrangement involves the loading of software onto the user's machine. This software cooperates with the filter list on the Content Manager's web server of the third party, as illustrated in figure 9. In this situation the third party has complete control over the user's Internet experience.

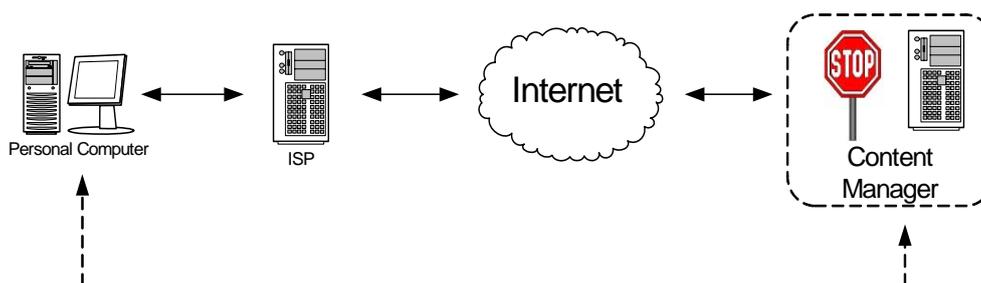


Figure 9 - Content filtering by third party, cooperating with client software

General limitations of filters

It is important to note that filtering software can help to keep users from being exposed to content that would not be suitable. Unfortunately filtering software is not without flaws and limitations.

Existing filtering and rating systems are sometimes unsophisticated, as users cannot be sure that content will be rated appropriately and that perfectly innocuous content will not be blocked. Examples of general limitations of filters are presented below.

- Filters are incapable of distinguishing between a sexual solicitation sent by e-mail and a news story about restrictions on online pornography or between a computer virus and a story about a computer virus. A nice example of this is the following:

Town gets caught in a porn-less Net¹⁸⁵

Blountsville Telephone Company CEO Rick Kiser But townsfolk like Chuck Harmon, who wanted to offer the town an Internet provider service decided to stop his service after a filtering problem. Citizens were livid when they logged on and found they could hardly get anywhere -- including eBay and other non-porn sites. Fifty-five percent to 65% of the Internet was totally gone after implementing strengthened filters to offer a porn-less Net. Kiser decided that if he couldn't offer quality service without pornography, he wouldn't offer it at all.

- Filters are easy to mislead. Some examples of sneaking past filters are:¹⁸⁶
 - ❑ David Carney's, writer of e-mail newsletters for Tech Law Journal, **misspells words** like sex (sez) and pornography (pormography) and camouflages the names of computer viruses to sneak past filters.

¹⁸⁵ Information retrieved from an article in USA TODAY, 'Town gets caught in a porn-less Net' written by Janet Kornblum (14/02/2002).

¹⁸⁶ Information retrieved from an article of The New York Times, 'Compressed Data: Law Newsletter Has to Sneak Past Filters' written by Pamela LiCalzi O'Connell (2/04/2001).

- ❑ Beaver College in Glenside, Pa., decided to **change its name** to Arcadia University, in part because some filters intended to screen out sexually explicit material blocked access to its site.
 - ❑ And recently, when the music file sharing peer-to-peer network Napster was ordered to block the access it provided to copyrighted music, some users began **renaming titles** in a form of pig Latin to confuse the filter.
 - ❑ Substituting numbers for letters and letters for numbers is an increasingly common practice.
- Using a filter may considerably slowdown the system performance.

'QuickPoll': an informal survey

In order to get an idea of the extent of the phenomenon, Unisys carried out an informal survey on its employees worldwide. This service is called 'QuickPoll' and is regularly used to ask any kind of question to all the employees of the company. For instance, there has been a 'QuickPoll' on the employees' habits regarding lunch time.

'QuickPoll' is accessed via the Intranet and people are free to participate or not. The procedure is very simple: all they have to do is read the question and check the box that corresponds to the answer they want to make. The metrics are calculated immediately and show the percentages of occurrence of the different answers, plus the total number of votes.

There is no classification whatsoever of the participants, so no indication of gender, age, role, or geographic location. The process is totally anonymous.

There is no control on the validity of the votes, however one does not expect deliberate cheating or incongruous votes; especially since nobody is obliged to participate.

The web site through which 'QuickPoll' is accessed is generally visited by 2000 or so employees, which is quite wide. 469 persons answered to our question, which represents a rather good participation rate, considering that the question itself entails a natural selection of those employees who surf at home via a private (non-Unisys) ISP. The reason for this restriction is that the access to the Unisys ISP is secure, much more secure than most citizens personal access to ISPs. The traffic is controlled to a certain extent and certain categories of material are filtered out by Unisys servers.

The question was 'While browsing the Internet on your home PC via a private (non-Unisys) Internet service provider, have you or your family ever been involuntarily exposed to child pornography material or solicitations?'. The possible answers were:

- Yes, even though we have an electronic filtering device on our machine
- Yes, but we do not have electronic protection on our machine
- No

This QuickPoll was published on the Unisys intranet on the 21st of March 2002 for a couple of days.

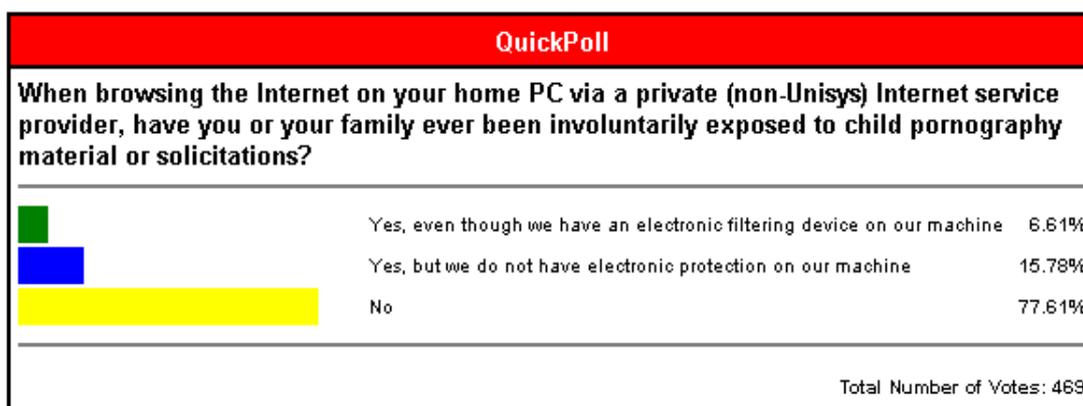


Figure 10 - Results of the Unisys intranet QuickPoll

As can be seen on Figure 10, the results show that among the 469 answers 22,39% reported to have indeed been involuntarily exposed to child pornography, around 3/4 had no electronic protection on their machine against 1/4 'protected' by electronic filtering device. These figures suggest two things: first the phenomenon is far from minor and, second, filtering devices do help reduce the access to such type of material.

Mapping of filtering software packages

Various filtering software packages exist on the market today. They differ in functionality, filtered categories, costs, ease of use, and quality of performance.

The most commonly used products today are presented in Table 2, together with their features and an indication of cost for a one-year usage. The major part of the information contained in Table 2 comes from an article published in a Belgian magazine for consumers' defence ¹⁸⁷. This information has been completed with information found on the Internet.

The information presented here is only descriptive. The evaluation will follow in the second part of this report.

¹⁸⁷ 'Test aankoop', March 2002, 'Wat glipt er door de mazen van het net?'

Product Brand and version	Lists visited sites	Restricts access to defined periods of time	Prevents sending out personal data	Checks e-mails	Checks e-mail attachments	Checks Newsgroups	Checks Chat sessions	Checks Downloading	Locking	Filters Bombs and explosives	Filters Hacking	Filters Hate and violence	Filters Drugs	Filters Religious extremity	Filters Pornography	Cost per year (Euros)
PERKEO++ Version 1.x	✓	✓	✓	✓	✓	✓	✓	✓	✓							619
McAFEE Internet Guard Dog Version 3.13	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	73,14
N2H2 Inc. N2H2 for home (Uke) a 1.0				✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	44
WE-WEBCORP.COM Web-blocker 2.0.1 Build 82	✓								✓	✓	✓	✓	✓	✓	✓	0
ONE LIGHT CORPORATION Bounce Version 2 pre-release	✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	44
SOLID OAK SOFTWARE INC. Cybersitter 2001.1.9.25	✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	55
WATCHSOFT INC. Disk Tracey KidWatch 3.1.10	✓								✓	✓	✓	✓	✓	✓	✓	55
VISIONSOFT Childlock 3				✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	45
SPY CATCHER CORPORATION Surin' Annette! N/S	✓	✓							✓	✓	✓	✓	✓	✓	✓	33
SYMANTEC Norton Internet Security 2001 3.0	✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	66,8
SURFCONTROL Cyberpatrol 5.00.002		✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	☐	64
S4F (SAFE 4 FAMILIES) INC. 6.03.4121						✓			✓	✓	✓	✓	✓	✓	✓	90
ICOGNITO TECHNOLOGIES LTD. PureSight Home 2.5	✓								✓	✓	✓	✓	✓	✓	✓	44
A.VALUE SYSTEMS Mom 1.38J	✓								✓	✓	✓	✓	✓	✓	✓	0
NET NANNY SOFTWARE INTERNATIONAL INC. NetNanny 4.1.0.0	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	57,1
OPTENET.COM Optenet.com client 6.6									✓	✓	✓	✓	✓	✓	✓	36,3
SYSTEMS CyberSentinel 2.0.5	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	38
8e6 TECHNOLOGIES X-stop 3.04							✓		✓	✓	✓	✓	✓	✓	✓	60
PEARL SOFTWARE Cybersnoop 4	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	55

Table 2 - Overview of filtering packages

The particular case of PERKEO++

PERKEO++¹⁸⁸ is a data scanner that searches for child pornography and animal pornography on any kind of digital media. PERKEO++ can search on local drives, network drives, news servers or web space. The discovered data material can be automatically deleted and the administrator informed to protect other people from that kind of material. PERKEO++ finds illegal pornography fast and reliably. Note that zoo-pornography is not illegal in all countries of the European Union.

PERKEO++ was developed in co-operation with the German BKA (Bundeskriminalamt, Federal Criminal Investigation Office).

PERKEO is used by German and international police departments since 1998. The program has been designed for performance, reliability and accuracy. In the mean time companies and universities like to use the software too.

PERKEO++ present the following features:

- The search library of PERKEO++ is updated continuously in co-operation with BKA;
- The search is extremely fast. Search speed achieves more than 100 MB/s;
- PERKEO++ can be applied to any local or network drive;
- PERKEO++ scans compressed archives too. (ZIP, ARJ);
- The configuration is simple and user friendly;
- It is integrated as a module;
- It requires nearly zero administration;
- It enables flexible control by scripts, and batch jobs are possible;
- The software is available for a multiplicity of operating systems. There are versions for DOS, Windows 95/98/NT/2000, Linux (Intel), Sun Solaris, AIX (power PC) and DEC Ultrix. Other platforms are on request;
- PERKEO ++ is suitable for all enterprises and institutions, for which the danger of storage or sending of illegal pornography does exist, namely:
 - Internet and E-mail Providers;
 - Free mail and Free space Providers;
 - Enterprises whose co-workers have an Internet access on a workstation;
 - Universities, vocational schools and other educational facilities;
 - Authorities and other organizations;
 - Prosecution authorities;
 - Automatic notification to criminal investigation departments is possible;

PERKEO++ does not guarantee a one hundred per cent protection against the spreading of illegal pornography. But resolute use of PERKEO++ at the hubs of the Internet would reduce this crime significantly.

PERKEO++ is not a crawler, which searches the Internet automatically. PERKEO++ will be installed preferably at hubs of the Internet – e.g. on a server of an ISP.

¹⁸⁸ PERKEO Data Scanner, Against Child Pornography and Animal Pornography <http://www.perkeo.de/>

PERKEO++ is not a real filter that automatically blocks files containing child pornography or animal pornography. PERKEO++ is a module that allows the reliable identification of inappropriate material. Based on the search results the necessary actions are made, e.g. deletion of the files or an automatic notification to criminal investigation departments.

PERKEO++ does not look for personal data.

The method used by PERKEO++ is generally well accepted and reliable. A hit is produced only if the digital fingerprint of a binary object is identical to the data stored in the search library. Pictures will not be included into the search library of PERKEO++ if they cannot be clearly classified.

Thus PERKEO++ is well accepted on German trials.

10.5. TRACEABILITY OF INTERNET ABUSERS

One way of reducing the spreading of unwanted material on the Internet is to install protective filtering devices that block the access to or the travelling of such material. But one essential aspect of the proliferation of illicit or dangerous material – but also behaviours – on the Internet is that the users have the feeling that they are completely anonymous; so that they can act with complete impunity. If it were possible to reduce this feeling of anonymity and impunity, no doubt the number of criminal acts and abuses mediated by the Internet would decrease.

The purpose of this section is to show that it is perfectly possible from a pure technical point of view to identify any user or machine connected to the Internet. However the legislation protecting privacy and free speech very often conflict with 'traceability'.

Most information in this section is based on the 'LINX Best Current Practice – Traceability' report: <http://www.linx.net/noncore/bcp/traceability-bcp.html>, when other sources have been used, it will be mentioned.

The ability to track down the originator an action on the Internet is usually called 'traceability'. This can be done by either by identifying the machine and eventually identifying the user.

This chapter is split into three different sections. The first one presents the different techniques and tools available to locate a machine, and explains how traceability can be achieved in e-mails, newsgroups and chat rooms. When the originator machine has been identified, the investigation proceeds to find out the user of that machine. The second section presents the different ways of identifying users. Finally the last section exposes the limitations to traceability.

Identifying the machine

Each time someone uses the services of the Internet, he leaves tracks behind that can lead back to him. The footprints are left by the IP address of the user's machine, which is unique. Internet Service Providers register IP addresses before letting customers use them to connect to the Internet.

Once connected, an Internet user gives that IP address to every Web page or Chat rooms he uses. It is also embedded in any e-mail the user sends or any newsgroup posting he submits.

Techniques and tools to locate a machine

There exist various different tools that can be used to identify and locate a machine that connects to the Internet. Once the IP address of a remote system is known with a sufficient degree of certainty, it is possible to identify the machine name, its location and owner. This is achieved first by checking appropriate registries to find the IP address, then executing a reverse DNS look up to have the name of the machine corresponding to that IP address. Finally trace route searches will help to actually locate the machine.

1. Registries¹⁸⁹

IP addresses can be checked in the appropriate registry, RIPE, ARIN or APNIC.

The name of the organization registered to be using the IP address can be determined by using the 'whois' tools to interrogate the registry databases that describe IP addresses allocations. The 'whois' tools can also report other information such as for instance, postal and telephone contact details.

There are numbers of programs and web sites dedicated to interrogating these registry databases that provide information about the ownership of an IP address or hostname.

The following URLs are all web sites that can provide information about the registered owner of an IP address.

- Check domain: www.checkdomain.com
- Allwhois: www.allwhois.com
- ARIN: www.arin.net
- Sam Spade www.samspade.org

There are also programs available on the market, that have the ability to process 'whois' commands. A few examples of such programs are: Cyberkit (www.cyberkit.net), Netscan Tools (www.netscantools.com), Neotrace (www.neotrace.com), AG Group Net tools (www.aggroup.com).

2. Reverse Domain Name System (DNS)

Once the IP address has been identified, it is possible to find the corresponding machine. The simplest technique for determining which machine corresponds to an IP address is to attempt a reverse DNS lookup.

The Domain Name System (DNS) is usually used to translate 'human friendly' names of machines into IP addresses, but it also supports a system to do the reverse, and translate an IP address into a name.

Some Internet applications may refuse incoming connections where there is no reverse DNS entry (i.e. where IP addresses are mapped to domain names, rather

¹⁸⁹ Extra information found at Random Art, an IP Tracking Tutorial, <http://www.random-art.com/tutorial/iptracking.htm>

than vice versa, using IP address written in reverse order), or where the forward and reverse lookups do not match.

3. Trace route

A trace route program is used to determine the path, across the Internet, to a specific machine. When investigating the path a trace route program provides, the machines close

to the first one are the most reliable, because the first machine, which is the actual originator of the 'abuse', might be forged, but the next machines in the path will most probably provide accurate information.

Trace route results can also provide the names of the ISP used for the connection. Contacting ISPs may be useful if it is impossible to contact the owner of the actual remote machine.

Trace route tools are easy to find. For instance, one can use the 'tracert' command in the Windows command prompt. Typing '**tracert [IP address]**' will provide the trace route results of the IP address entered.

Here follow examples of organizations that also provide trace route tools.

- SamSpade

SamSpade is a free integrated network query tool for Windows. It has a very good quality set of tools including 'whois', trace route, ping, nslookup, dig, finger etc. (See www.samspade.org).

- Visual

Route

Visual Route is a Trace route application.

E-mail Traceability

An E-mail is made traceable by virtue of headers placed into the e-mail as it passes through each system. These headers are placed at the top of the e-mail. Reading the header downwards, it is possible to work back in time towards the original source¹⁹⁰.

A header can be broken into different sections of information, called header lines. An example of a typical header line is:

```
Received: from forged.and.invalid (really [192.168.0.1]
by mail.example.com with SMTP id 123BDC4
for recipient@pop3.example.com ; Sat, 09 Apr 2002 01:00:00 -0700
```

As an e-mail is passed from machine to machine, extra 'Received' header lines are added. These lines were originally invented to allow problems with the e-mail system to be tracked down, but they can also serve as a way to trace the path that an e-mail has taken. This path can lead to the original source of the e-mail.

In the example above, the e-mail was sent from [192.168.0.1], which declared itself in the SMTP protocol HELO message to be the host 'forged.and.invalid'. HELO is a command within the SMTP e-mail protocol, used to announce the name of a remote

¹⁹⁰ More information can be found on <http://www.usus.org/elements/tracing.htm> and on WeirNet Tracing Email / How Spammers Find you <http://www.weir.net/WeirNet/support/faq/antispam/tracing.html>.

machine. The e-mail was received by the server 'mail.example.com' and the local logs on that server will refer to the message under the identifier '123BDC4'. The e-mail was timed to have arrived at 1 o'clock on the 9th of April 2002 and it was addressed to recipient@pop3.example.com.

Since a person who misuses the e-mail system may generate fake 'Received:' headers, it is very important that every e-mail handling system adds its own header. The difference between the valid and invalid headers will then become clear, and the source of the e-mail can be identified with certainty.

Correct configuration of headers is thus very important for traceability reasons. Note that it is important for the 'Received:' header to record the IP address of the sender, because the IP address is the only piece of information that cannot be easily forged. It is also necessary to clearly identify the e-mail-handling machine that is adding the 'Received:' line. This means placing a fully qualified domain name into the header.

Another configuration issue while creating headers is to record an accurate time and date. The time must be configured correctly so that the correct time zone is given.

Most mail readers do not show the header because it contains information that is for computer-to-computer routing. The e-mail program usually only shows the subject, date and the 'From' / Return' address of the e-mail.

But the header can usually be shown in the e-mail client. The method is different according to the e-mail program. For instance,

- In Netscape mail: the user goes to the 'options' menu, chooses 'show headers' and 'select all'.
- In Microsoft Outlook this tool is found in the 'tools' menu, then the user chooses 'options'.
- In Eudora for the Macintosh or IBM, one has to press the button labelled 'Blah Blah Blah'.
- However, there exist programs that do not comply with any Internet standards (such as cc-Mail or Beyond Mail), which throw away the headers. So nobody will be able to get headers from e-mail messages sent by such programs.

Newsgroups traceability

Like e-mail messages, the articles posted in newsgroups also contain a header that provides the necessary traceability information¹⁹¹.

The headers of news articles are called NNTP-Posting-Host headers as the newsgroups use the Network News Transfer Protocol.

For instance, here follows a forged newsgroup header:

¹⁹¹ The information in the following two sections is based on information from the House of the Dead web site: <http://www.houseofthedead.org/> and additional information has been provided by mail by the organization. Extra information has been found in Chat Wise, Street Wise - Children and Internet Chat Services, A paper prepared by the Internet Crime Forum IRC sub-group

http://www.internetcrimeforum.org.uk/chatwise_streetwise.html.

Newsgroups: alt.some_group, alt.another_group
Subject: This is a badly forged message!
Date: Mon, 1 Jan 2002 10.00.01 -0000
Lines:
X-Newsreader: My Special Newsreader
X-MimeOLE: Produced by MyMimeOLE 1.1
NNTP:-Posting-Host: mydialup.xxx.org
Message-ID:
X-Trace: 1 Jan 2002 10.00.01 -0000
Path: news.mynews.org!newshub1.mynews.org!mydialup.xxx.org
Xref: newshub1.mynews.org alt.some_group

'X-trace' is an additional header line now commonly added by news servers. It will usually include the name of the news sever where the article was injected, the time of injection and the IP address of the machine the article came from.

There is also a 'Path:' line in the header. This line contains the list of all the hosts that the message traversed. Unlike an e-mail message, a news article is transferred across multiple networks, each host generally performing its own form of logging.

By tracing the path of each entry in the 'Path:' entry of the message header, it is possible to determine the originating host. If an entry seems to be faked, the nearest good host will be analysed.

To be able to control the abuse of newsgroups it is essential to ensure that the originators of the articles can be traced. Unfortunately there are no formal standards for these headers at present.

The information that such headers must provide is an IP address and a timestamp, which is provided by the X-trace line in the header. Timestamps are required to disambiguate IP addresses. The most accurate way to record current time is to use the Network Time Protocol (NTP).

Like for e-mail traceability, it is important to ensure that any domain name that is being used is valid, and recording IP addresses is encouraged.

IRC traceability

IRC is seen as the heart of child pornography online. Many paedophiles and child pornography traders communicate and spread their material via IRC. Paedophiles sometimes hang around chat rooms to lure children into their sick conversations about their sexual desires.

Tracing child pornographers on IRC however is very difficult and time-consuming. The best way to find child pornographers on IRC is by monitoring IRC. There also exist search applications, but they are not very effective.

1. Monitoring IRC

The best way of finding child pornographers on IRC is by monitoring IRC. This means long sessions of sitting, waiting, and watching chat rooms for signs of a lurking child pornographer. It is a difficult and time-consuming activity.

Most often, this form of searching is fruitless, and is sometimes seen as a waste of time. There are occasions, though, that monitoring IRC rooms can be rewarding, especially as a step is reached into the world of private communication.

Trust is the most important issue in these rooms, and that is hard to obtain without actually showing off a product.

The best method to get into contact with a child pornographer is to pose as a teenager or a child looking for a chat. While monitoring, having patience, integration with the room and its culture, and being persistent are very important aspects. The more often a person is 'seen' in a room the more likely it is that someone will eventually approach that person for a private session.

2. Applications

There exist applications in which keywords trigger some alert of action. These applications examine the written communication in a chat room. When it encounters a keyword that exists in the keyword list, the application triggers a message. These are actually a kind of keyword filters.

Unfortunately such devices are easily fooled by letter substitution. And the letter substitution technique that IRC child pornographers use would require an extremely advanced application, able to understand this language. For instance, here are several ways that child pornographers use to spell the word 'Lolita':

- L0l1t@
- 1011ta
- !o!it@
- L_o_l_i_t_a

Moreover speech over the Internet, also called 'net-speak' is now possible using a microphone on the computer. Child pornographers who use this technique are even more difficult to detect.

3. Tracking people on IRC

Tracking people on IRC is possible because IRC clients are built with the 'whois' command. In much the same way as the reverse DNS technique allows to relate an IP address to the corresponding domain name, the 'whois' command allows to make the link between a nick and the corresponding IP address. It is also possible to discover a suspect's IP address if he has recently changed his nickname. This is possible because most IRC operators temporarily store information regarding nicknames versus IP addresses.

IRC operators can be a source of evidence too, as they should maintain logging facilities on recent sessions. This logging information includes:

- The IP address of the machine from which the user connected to the server.
- The time a user connected to the server.

- The amount of time the user remained connected to the server.

In order to provide a better traceability, though not always done, the following information needs to be logged:

- The time at which the user joins and leaves each channel of the IRC network.
- Any times at which the user changes nickname, and what is his new nickname.

Identifying the user

Identifying users is more difficult than identifying machines.

Checking names and addresses, credit cards, telephone numbers is usually not possible because the child pornographers want to maintain their anonymity. They know they do illegal things and they use every available means to avoid being caught. Changing their personal data by using aliases and forged data is of course easier than forging IP addresses for example.

Since each connection to the Internet has to go through an ISP, every user needs an Internet account at an ISP.

In the past, subscribing to an Internet account used to be only possible by paying a monthly fee. This meant that the users had to reveal themselves to hand over their dues. They could enter fake names and address data, but their credit cards number had to be correct. These 'pay up' ISPs would not offer accounts to unidentifiable people since this would have impacted whether or not they were likely to be paid.

Free trials have been provided by the ISP industry for some time, but the recent trend is to provide accounts for free in perpetuity.

However, these free services must still manage to achieve traceability or at the very least be able to detect the return of a user who has previously misused their system. A Best Practice at the moment is to require that the Calling Line Identification (CLI) be available, or that there exists some kind of relationship with the users that would allow traceability.

There are solutions but they can only work out if all ISPs cooperate. If all ISPs registered a certain amount of information on the persons to which they provide an account, this would increase traceability.

1. User identification by name and address

The simplest way of identifying a user is to ask them their name and address. The vast majority of users will provide valid details.

But there will always be people who will attempt to fake their credentials. These misleads may be detectable by data validity checks. It is possible, for example, to use standard databases to check that the house number and street name correspond to the postcode that has been provided.

2. User identification by credit card check

It is common to insist that holders provide a credit card number before their account is activated. If the account is to be paid for, there is an obvious reason for doing so. This creates thus a link between the Internet account and the real world.

The mechanism is not infallible since lists of stolen cards circulate on the Internet. Even formulas for creating apparently valid credit card numbers are widely published. To investigate whether the number is forged, one has to check with the credit card company. Organizations do exist that handle this type of validation for a fee.

Note that today free connections to the Internet are provided by ISPs. Checking a bank account is not possible this way.

3. User identification by telephone call back

If the user is called back on the telephone before activating the account, this would provide some assurance that they can be contacted again. Unfortunately this action is very labour-intensive and therefore usually not done.

A similar solution would be to require the user to provide a fax number for contact. This can be useful in business transactions. However, for private users this is not always possible, as not everyone owns a fax machine.

4. User identification by client certificates

The availability of cryptographic digital certificates provides a possible future solution to the problem of user identification.

A cryptographic digital certificate is a digitally signed statement that contains information about an entity (which can also be a person) and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization called a Certification Authority (CA), after the CA has verified that the entity is who it says it is.

Certificates can contain different types of data, for example the format of the certificate, the serial number of the certificate, the name of the CA that issued the certificate, the name and public key of the holder, the CA signature and the document expiration date.

The ISP could only accept account applications that were digitally signed by the user and rely on the promise by the issuing authority that the certificate belonged to a traceable individual in the real world.

This system is not widely used today, because of its high costs, reliability problems due to the absence of a standard, and the lack of any worldwide common legislative framework.

5. User identification by Caller Line Identification

Calling Line Identification (CLI) provides the number from which a telephone call is made to the destination equipment. A telephone company will usually be able to map this number to an actual physical location. The ISPs equipment can also record the CLI and in principle it provides the phone number that made each individual call to the ISP.

Most telephone companies have access to two types of CLIs. One is the 'user' presented CLI and the other contains an 'engineering' CLI plus some extra information stating what may be done with the user CLI. The CLI is a valid number or a valid partial number.

Telephone companies use the 'engineering' CLI because this is the only method of calculating charges between them. ISPs, which are usually not telephone companies, are only able to access the user CLI.

Normally all telephone calls should accurately carry the CLI of the calling party. Unfortunately this is not always true and this technique presents significant limitations because

- the user may have requested the phone company to withhold CLI.

Even if CLI is not suppressed for all calls, dialling a special number will disable CLI for an individual call. The CLI is still available to a phone company in an 'engineering' form, but not to an end system, such as an ISP.

- CLI information is not always passed reliably across net boundaries.

It is for example unusual for trans-Atlantic calls to have any CLI. It can also happen that the CLI fails to travel between various networks with any reliability.

- the CLI provided may be generic.

One of the side effects of using some discount phone schemas can be that the call appears to originate from the discount provider rather than from its true source. Therefore traceability will depend upon how much logging has been enabled within the third party system.

The CLI can also belong to a company, with many users dialling out through an individual extension. Traceability will then depend upon what types of records are kept of usage by a particular phone extension.

In order to gain traceability, ISPs who are providing 'free' services could require that CLI be presented before calls are accepted. When abuse has occurred no further accounts can be opened or operated by calls that originate from the same CLI. However, the ISPs who provide 'paid' services tend not to require CLI since they gain traceability by the credit card number identification of the users.

The limits of traceability

Investigating on the machine involved in Internet services abuse is feasible in theory. However in practice, there are a lot of limitations to traceability. As will be explained hereafter, there are different ways of connecting to the Internet and each way has its own limitations in providing traceability¹⁹².

Dialup Access (Modems and ISDN)

Dialup access is one of the most common forms of access to the Internet and there are many ISPs offering this type of connection.

A communications link is made over ordinary voice telephone lines (analogue of digital) using a modem or ISDN terminal adapter. The session starts with the user authenticating him to the ISP, usually by a simple password. The user's machine is then given an IP address and connected to the Internet.

There are three main ways in which it is possible to associate a dialup connection to a particular individual. One can examine the credentials that were given when the

¹⁹² More information on this subject can be found in the article 'The limits of Traceability' written by Richard Clayton: http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

account was registered. One can use the CLI to determine the source of any particular call within the telephone network. And maybe one could use digital certificates in the future.

As already discussed in the previous chapters of this report, each of them has its own specific limitations.

Nowadays 'free' Internet accounts are available and thus traceability to the individual through credit card identification is no more possible. With credentials becoming increasingly dubious as an identification mechanism, one can use CLI information for traceability. However, as explained above, CLIs also have significant limitations.

But it should be noted that it is, in principle, possible to determine the origin of a dialup call even in the absence of a CLI. The telephone company involved will have billing records that include every single call and with accurate time and duration information per call.

New Technologies

Today a number of relatively new technologies exist for providing access to the Internet.

- High-speed access to the Internet is becoming available over phone lines or cable networks, such as ADSL and Telenet that are available in Belgium. More and more people start using this way of connecting to the Internet because it is faster and in some cases cheaper than using a dialup connection.

Finding the individual behind a connection to the Internet with these new technologies can be done in the same three ways used in the case of dialup access. But in this case the investigation of credentials may be more effective because the use of these high-speed connections is not free and thus 'real' information has to be provided in order to charge the users. Naturally, there could still be impostors using somebody else's account and password for connecting to the Internet.

Investigating billing records on lower volume systems, such as ADSL network, is easier and can be executed cost-effectively.

- Nowadays Internet access from mobile (cell) phones is also available. It is possible to plug in a laptop into a cell phone, or with the current WAP system; the computer may be within the phone itself.

The traceability of dialup access to the Internet from a mobile phone is accompanied by the same set of problems that can occur while identifying the identity of the abuser using a fixed dialup access account. There is, however, an extra difficulty when 'prepaid mobile cards' are used. In many countries there are no registration requirements for the ownership of 'prepaid mobiles cards'. The call minutes are bought in advance and both phones and cards containing time can be purchased for cash. Therefore, even if the phone number is available, there will be no record of the identity of the owner. Technology does exist for determining the physical location of the phone, but the accuracy of this is limited. In practice, most traceability for prepaid phone is done by investigating the billing records of the card. With these records it can be possible to identify the abuser from the persons he has been in contact with.

Leased Lines

A leased line is, in general, a permanently configured pathway across the telephone company network from the customer to the ISP. Companies usually use these leased lines. In the company itself the line is used by different workstations and thus divided into many smaller connection lines.

There are two ways for allocating IP addresses at the customer's site:

- One is allocating a subnet, a group of 2, 6, 14, 30, 62 ... addresses of which one is used for the customer 'router' and the others are available for individual machines.
- The second scheme is called NAT (Network Address Translation) where a single IP address will be visible to the Internet. A specialist machine on the customer's side will keep track of all open connections and will distribute incoming data to the appropriate customer's workstation.

When investigating abuse events where a leased line is involved, one will need to determine which workstation at the customer's end of the leased line is involved in the events that they wish to investigate.

The basic difficulty is that the logging records at the ISP will ensure that events can be traced to the leased line, but the records will not usually be able to distinguish between the different machines at the customer's site.

In principle, determining the workstation that is of interest from the open Internet onto the private IP network is possible. However, there are a number of practical difficulties with this:

- The first one is that the customer may not keep sufficient logging records. Records need to be kept of who used which IP address from when to when.
- Even if these records are logged, then there is still the problem of 'hacking'. Technically competent people may be able to 'hide' themselves in such a way as to incriminate an innocent user by using his machine.

Using Anonymous Machines

Since tracing is possible in a lot of cases, some people use a machine other than their own, in order to remain anonymous.

- 'Cyber cafés' are perfect to stay anonymous on the Internet. These cyber cafes usually do not keep logs of the identity of those who used a particular machine. There is of course the risk of being remembered by the staff of the cyber café, but this risk is minimal.

Cyber cafes are not unique in providing public access points. One can often find machine in libraries, hotel lobbies or in schools.

In order to provide traceability it is of course important to keep logs of who used the machine from when to when.

- Some people may use a machine without permission, remotely operating it. These people are often called hackers. It is very difficult for investigators to find them.

If the events being investigated are stopped and the local records have been removed then it is almost impossible to trace the abuser.

If on the contrary the events are ongoing, then it is still possible – with the help of the owner of the machine or the network administrator – to determine the IP address of the hacker.

Conclusions on the mapping

Can technological devices completely protect people against child pornography on the Internet?

No, but the spreading and the exposure to child pornography on the Internet can be limited by the use of the available technological devices.

People can protect themselves and others who fall under their responsibility, against the exposure to inappropriate material by the use of filter software packages. However, the filtering packages available on the market today are not a foolproof protection against inappropriate material. They cannot guarantee to block all child pornography material that is spread through the Internet and they even cannot promise not to block perfectly innocent, informative material.

Catching and punishing people who abuse the services of the Internet will also decrease the spreading of child pornography on the Internet. Therefore the person behind the material needs to be identified. Today various tools are available contributing to the traceability of these child pornographers. However, different limitations are encountered when tracing the abusers. These people are smart and use every tool and backdoor available in order to keep their anonymity. Another limitation is that given the lack of appropriate and common legislation, and the high cost of logging and archiving these logs, the information that would provide traceability is usually not available at the time of investigation.

Further development of technological devices, extra regulations and the creation of standards are necessary in order to improve the protection against child pornography material.

10.6 EVALUATION OF EFFECTIVENESS OF TECHNOLOGICAL MEASURES TO TACKLE CHILD PORNOGRAPHY ON THE INTERNET

The purpose of the present document is to provide a set of parameters or selection indicators that used in combination with one another enable any party concerned with the problem at hand, to make a knowledgeable choice among the different preventive technological devices or approaches available.

These parameters are not strictly speaking 'efficiency indicators', because for the issue at hand, what is efficient in some circumstances is not so in others. However they are linked to the efficiency because they allow making the most appropriate choice considering a series of relevant factors. In this respect they satisfy the requirements of the study.

The scope of the present report covers a set of parameters or selection indicators, their justification of use, the advantages and disadvantages of the different possibilities according to context and purpose.

The study ends with an overview of how these indicators are represented in a sample of products available on the market.

Structure of the document

The present document starts with an introductory section that briefly describes the context, purpose and scope of the study and the structure of the present report. It then presents shortly the method of data collection and ends with a list of acronyms. The document is then structured in three more sections.

Section 2 is devoted to presenting a list of selection criteria or indicators for choosing the right protective device(s) according to the context and purposes. The section provides a description of each indicator together with their various options and related advantages and disadvantages.

Section 3 gives an overview of existing products and Section 4 draws the conclusion of the report.

The products specifications sheets, or lists of features, that were drawn for making an overview of existing products constitute the Appendix 1. Appendix 2 is provided for illustration purposes and consists in an example of a rating system.

Method for data collection

The investigated data in the report was collected through:

- The Internet;
- Information received from contacts with other organisations that fight against child pornography on the Internet;
- Information received from manufacturers of technological devices;
- Magazines that have published information about the prevention of child pornography

10.7 CHOOSING THE RIGHT PROTECTIVE DEVICES

Today a variety of preventive technological approaches are available to protect Internet users from undesirable and even harmful material. They can be deployed both at the Internet Service Provider (ISP) level and/or at the client level, such as homes or schools.

ISP control mechanisms have significant promise in providing content management, especially if they place some additional control in the hands of users (supervisors), as they are the ones who know what they want to have filtered for their 'children'.

These mechanisms provide a more technologically robust system upon which parents can place greater confidence than desktop filters. ISPs have all the necessary technical skills in the house; they can better focus on the latest technologies and be up-to-date at all times.

Although desktop filtering technologies may be more prone to tampering, they allow users to control the content at a finer level than would be expected from an ISP.

These technologies however are not 100% effective as computer-adept people can easily circumvent them. Furthermore they are not fully reliable as they cannot effectively filter all undesirable content and as they may also filter out some desirable and educational content 'unintentionally'.

Whether the control is managed remotely at the ISP or locally on the desktop, transparency and knowledge of the mechanisms deployed is important. The user needs to understand what is being filtered, when it is being filtered, and why it is being filtered. But control mechanisms are difficult to maintain in the existing anonymous Internet environment, in which new material is constantly being added, and new web technologies continue to be developed and improved.

In order to operate efficiently and to deal with the difficulties related to the Internet, these control systems must acquire and maintain, over the long term, accurate knowledge not only about the different available web sites and web pages, but also about the different users.

Regarding the shortcomings of the technologies available today, we have to bear in mind that it is better, particularly for young children, to miss some harmless material than to be exposed to offensive material.

Indicators Description¹⁹³

With the help of the public information available, we have selected the following set of indicators, which according to the option chosen (i.e. their value) and combined appropriately to each purpose and context lead to an – as much as possible– efficient protection.

- Type of protective device (specific browser, filters etc...)
- Scope of the protective device
- Location where the device is installed (ISP, personal computer)
- Architectural choice for ISP located protective devices
- Type of technological approach for content control
- Quality of filtering
- Management of information control
- Configuration and user-friendliness
- Security

¹⁹³ The list of selection criteria provided in this chapter was partly built by using information from: CSIRO, Commonwealth Scientific & Industrial Research Organization – Access Prevention Techniques for Internet Content Filtering – Prepared for the National Office for the Information Economy – <http://www.cmis.csiro.au/Reports/filtering.pdf>

Test Aankoop – Nr. 452 – maart 2002 Test van 18 internetfilters – Wat glipt er door de mazen van het net?

Shining a light on Filters in Libraries by Karen G. Schneider MSLIS – <http://www.bluehighways.com/filters/filtersc>

The book 'Youth, pornography, and the Internet' written by Dick Thornburgh and Herbert S. Lin in which dimensions of choice identified by GetNetWise are quoted.

An ethical framework: Mechanisms for user enabled choice and normative claims. http://webworld.unesco.org/infoethics2000/documents/paper_conley.rtf

- System requirements
- Assistance (Support)
- Financial cost
- Future perspectives

These indicators together to the different options available for each of them and are described in the dedicated subsections below.

Type of protective device

The market today offers the following types of devices. Some products even offer combinations of several different types.

- Special purpose browsers for children

These are browser applications that are targeted to child users. Such applications can provide easier search strategies and friendlier graphics, remove advertisements, and provide filtering and search-safe domains in a way that makes it fully transparent to the parents. They can be fully aware of the information their children receive and have trust in the appropriateness of the information.

- Special search engines and portals

The idea behind both special purpose search engines and portals is to use a third party gateway to provide access to Web content. These portals are web access sites that try to provide a domain of desirable sites for the user to explore. As long as the user comes in through the portal, they view a pre-selected domain set of the web that excludes undesirable and harmful material. The special search engines do the same by listing only results of sites that do not contain objectionable content.

- ISP applications

Some ISPs offer services designed especially for children. ISPs may provide filtered Internet access or restricted access to chat rooms, newsgroups, or other types of services. They usually do this by providing a selection of user profiles with a different type of control adapted to diverse age groups, such as 'children -6', 'children -12', 'youngsters' and 'adults'.

There exist also different types of special proxy¹⁹⁴ applications that can be added on ISP level to remote server proxy modules, and allow the execution of content control. Technologies, such as URL filtering and keywords filtering, control the clients web requests and responses.

- Restricted access applications

These applications reside on the host site and restrict access to services or data on that site only to authorised users. Different types of authorising methods are used. Data can be encrypted and thus only authorised people will be able to decrypt the data. The authorisation can also be achieved by providing passwords or by checking credit card numbers. The credit card number can also be used for age verification, in order to validate if the visitor has the appropriate age to

¹⁹⁴ For definitions and descriptions of technical IT terms, see the annex 1 of the September 2002 intermediate report.

see the information. New biometric algorithms and hardware devices are being developed as well, to uniquely identify users using, for example, smartcards¹⁹⁵, finger scanning, retina scanning, voice print, even user's individual typing rhythm.

The best-known example of uniquely identifying users by individual typing rhythm is BioPassword. The patented BioPassword¹⁹⁶ keystroke dynamics technology uses a proprietary algorithm to make biometric measurements of a keyboard user's individual typing rhythm. The technology can be adapted to any application that utilises a keyboard or keypad.

- Personal computer applications (Filters)

These services or systems, as the name already states, can be placed on personal computers for controlling the email, controlling access to ftp sites, telnet hosts, discussion and chat groups, and newsgroups.

Some applications focus on one or a small number of these options, while others are broader applications, which provide a large package of services and are commonly called 'Filters'. Filters are the most-used technology-based tools.

Placing control mechanisms on personal computers can facilitate their configuration and reconfiguration by parents, teachers, or other administrators. On the other hand, it may also facilitate the reconfiguration of these mechanisms by children, against their parents' wishes and possibly without their parents' knowledge. Therefore some of these PC-based products have been designed with mechanisms to prevent tampering. Furthermore many PC-based products require frequent updates, but fortunately some can update themselves automatically when the PC is connected to the Internet.

Scope of the protective device

Internet¹⁹⁷ content is provided through a variety of protocols including HTTP (Web sites), FTP, newsgroups, chat, telnet, peer-to-peer, and email.

Some products and services focus on one or a small number of these protocols, while others provide more comprehensive solutions, monitoring everything an individual does online.

In addition, some products and services monitor only incoming communications, while others monitor both incoming and outgoing communications. Tools that monitor outgoing communications can often be configured to prevent children from giving out personal information that could be used to harm them such as their

¹⁹⁵ A smartcard is a small physical hardware device (typically the size of a credit card) containing read-only non-volatile memory and a microprocessor that can be inserted into a card reader attached to a computer. In most scenarios, the individual user carries the card and inserts it into an Internet access point that requires such a device. The memory which is on the device can store information about the user, including his or her age, preferences for material to be blocked, and so on. Software installed on the computer, and on Web sites visited, would check the smart card for dates of birth when necessary, and if the user were underage for certain types of material, would refuse to grant access to that material.

¹⁹⁶ For more information about BioPassword, visit: <http://www.biopassword.com>.

¹⁹⁷ Internet versus the WWW, the two terms are not synonymous and should not be confused. The World Wide Web is one of the ways that information can be transferred over the Internet. The Internet, not the WWW, is also used for e-mail, Usenet news groups, instant messaging and FTP. So the Web is just a portion of the Internet, although a large portion.

home address or phone number. Email control applications can focus on email spam¹⁹⁸, and the addition of attachments as well.

Location where the protective device is installed

Preventive technological devices can be installed at different levels, namely at the ISP's, at the end user's level, or at times at both.

- **End user:** The software operates entirely on the end user's PC, along with associated control lists.
- **Server or ISP:** With this type of application, the controlling takes place at the server level, either within a corporation or on an ISP's server. No special software is required on a user's PC.
- **ISP and User:** With this type of software the control takes place on a server, generically operated by an ISP. The end user, however, is required to load special software, typically a replacement browser, which cooperates closely with the remote server.

Providing Internet control at ISP level however can require expensive specialised switching hardware and multiple filtering servers.

The hardware and software that is most commonly used to provide filtering by ISPs in fact have not been primarily designed for this purpose, but were in the first place used in order to isolate private networks from the public Internet, or to improve performance and reduce costs by 'caching' web content.

Architectural choice for ISP located protective devices

The different types of architectural technology that ISPs could use for filtering are:

- Conventional proxy servers;
- Transparent proxy servers;
- Specialised cache engines.

1. Conventional proxy servers

Proxy servers are a kind of secure gateway between the Internet and private networks. They can be configured to filter requests and responses.

Conventional proxy servers sit directly in the path between users and the Internet. Consequently, all ISP clients must configure their browser software to point to this proxy server to pass all web traffic to the proxy rather than sending it directly out onto the Internet.

Figure 1 shows the traffic flow when a user accesses the Internet through a conventional proxy server.

¹⁹⁸ Spam is a flood of copies of email messages, which is a mechanism that is commonly used by spreaders of objectionable material. Spam control uses rules to scan the headers of incoming messages to eliminate likely spam messages.

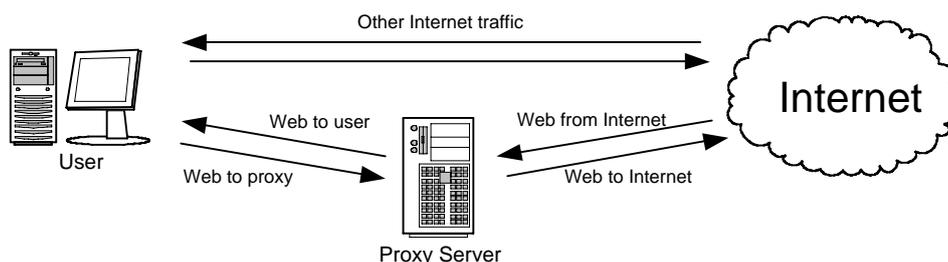


Figure 2: Use of conventional proxy server

2. Transparent proxy servers

Transparent proxy servers are designed to avoid the required users' configuration of conventional proxy servers. They take on the roles of routers or gateways in the network. Browsers send request messages onto their local network and these will be routed through the transparent proxy at some point on their path to the Internet.

By the way, this implies that all traffic must pass through the proxy even the information that does not need to be filtered.

Figure 2 shows the traffic flow when a user accesses the Internet through a transparent proxy server.

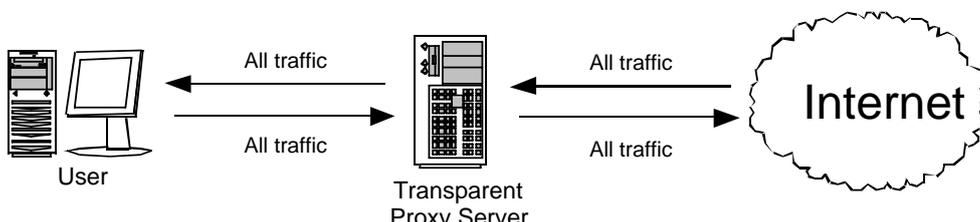


Figure 3: Use of transparent proxy server

3. Specialised cache engines

These high performance caching and filtering systems use special purpose routers or switches to divert only the web traffic that needs to be filtered, to the cache or filter. Any other traffic passes directly to the Internet.

Figure 3 shows the traffic flow when a user accesses the Internet through a specialised cache.

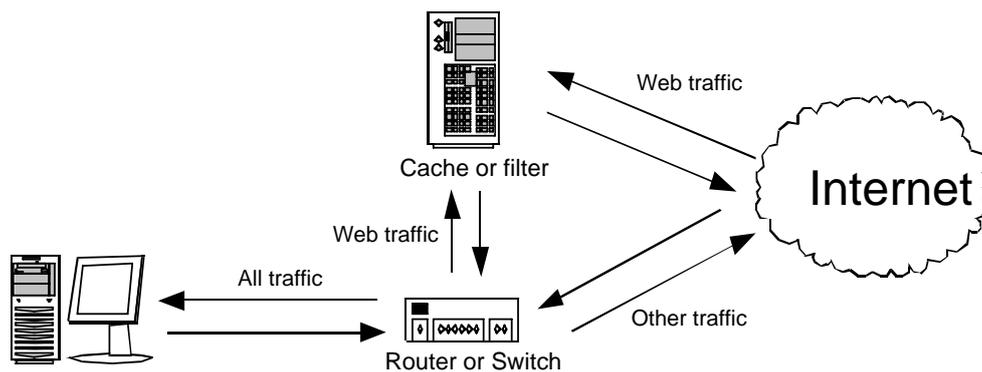


Figure 4: Use of a specialised cache

Type of technological approach for content control

There exist several technological approaches for implementing the control of the information visible to the user, or to the individuals under the users' supervision.

The following technologies are widely used by many companies. Some are used as a stand-alone method; others are used in conjunction with each other.

Controlling can be done in real-time and a-priori. Site labels and URL lists are a priori methods; the analysis is done beforehand, whereas the image analysis and text analysis are real-time analysis methods. The rules and specifications used for real-time analysis must still have been defined in advance. The techniques used for email control, IRC, newsgroups, etc. and monitoring are always real-time methods.

Site Labels or rating systems¹⁹⁹

Rating systems are in fact series of categories and graduations within those categories. Each category describes the nature of the content such as 'Race', 'Sexual content', etc. Within these categories further specifications are made such as 'Romance, no sex', 'Explicit sexual activity', or somewhere in between. The web sites are labelled according to the categories the contents belong to.

Individuals and groups can develop rating systems by defining categories and subcategories. PICS²⁰⁰ is an organisation that enables anyone to create rating systems. PICS is the framework for rating systems, not a rating system in itself. Appendix 2 presents the SafeSurf's rating systems, as illustration, which is built on the PICS platform.

Online rating systems work in a variety of ways. Some use a system similar to television or movies, and label Web sites according to age-appropriateness. Other use labels or seals to identify approved Web sites. Most systems work with web

¹⁹⁹ See also Section 10.2.1 of the September 2002 intermediate report; and Jacob Palme 'Choices in the Implementation of Rating' available on <http://www.dsv.su.se/~jpalme/select/rating-choices.html>

²⁰⁰ The World Wide Web Consortium's (W3C) Platform for Internet Content Selection - 'PICS' is an infrastructure for associating labels (metadata) with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing, privacy, and intellectual property rights management.

PICS official website: <http://www.w3.org/PICS>

browsers or filtering software to block sites that have been identified as inappropriate.

There are 2 main methods of using rating systems:

❑ **Self-Rating**

In this method publishers of a site can evaluate their own web site by using available rating systems.

❑ **Third-Party-Rating**

Here third parties such as organisations and groups evaluate the web sites of individuals and indicate labels to the content.

Third-Party-Rating Methods

Third Parties typically use a variety of methods to efficiently rate a web site.

At this time there is no single and perfect methodology of web sites rating definitions, which would effectively reflect the value of the site from an average user's point of view.

Each of the methods has its drawbacks, though in general they give a rather objective view.

The following rating methods are commonly used:

❑ **Link popularity rating**

Calculating the amount of links from other sites to the one that has to be rated.

This is a rather good and objective method, though it is useful only for considerably popular sites.

❑ **Visits counting**

Counting the amount of visits of the main site page or even all pages using graphic counters – most frequently used by Internet rating systems.

Counters more often reflect popularity than appropriateness of a web site. Another problem with counters can be called reverse influence. Which means, the higher the resource is placed in visits-rating lists, the higher is the amount of users attending it, which in its turn increases its rating.

❑ **Click lists**

Counting the amount of clicks on sites links from directories, for example from search engines.

Rating by clicks on site link in directory defines popularity of resource only from the directory users point of view and does not take into account users who already know this site or have saved its address in bookmarks (favourites) as well as coming from other sources.

❑ **Voting**

This means taking into account voting and users appraisal of sites of users.

Voting partially reflects users' opinion, but many users in favour and with 'interest' in the site tend to come back and vote for it. Usually site owners do this.

❑ **Personal rating definition criteria**

Personal rating definition methods are very subjective. Such methods consider not only popularity, but also usefulness of a resource. In such case informatively interesting and not sufficiently promoted or poorly designed site can have the same rating as widely promoted, professionally designed site with pale content.

Existing rating software and services

There are several rating systems in place on the Internet. Most use a system of technical specifications known as PICS to rate their content.

The following list is a summary of the most commonly used rating systems. Web sites rated with any of the following systems can be recognised by the appropriate logo, which is displayed on their home page.



The ICRA (Internet Content Rating Association) is an independent international organisation that rates Internet content. The system labels sites using broad categories including chat, language, nudity, sexual content, violence, gambling, drugs and alcohol. Internet Explorer is currently designed to block sites using ICRA ratings.



The RSACi system, which is now administered by ICRA, has also been a well-known rating system. But in order to be more effective the RSACi rating system has currently been phased out and replaced with the ICRA rating system.

For more info: http://www.icra.org//_en/



ESRB provides ratings for Internet Web sites, chat rooms, bulletin boards and multi-player games. The Entertainment Software Rating Board (ESRB), the same body that rates video and computer games, administers the ESRBi system. Internet Explorer is designed to block sites using ESRBi ratings.

For more info: <http://www.esrb.org/>



SafeSurf was the first rating system on the Internet. SafeSurf uses a 12-category system to rate Web sites according to age level and content. Both Internet Explorer and Netscape are designed to block sites using the SafeSurf rating system.

SafeSurf is a PICS-compatible rating system.

For more info: <http://www.safesurf.com/>



TRUSTe identifies Web sites that comply with acceptable privacy guidelines. A TRUSTe 'kids- seal' is awarded to children's Web sites that obtain verifiable parental permission before collecting information from children, and also inform parents how the information will be used.

For more info: http://www.truste.org/programs/pub_child.html

Lists of URLs

The most frequently used content control mechanism is 'URL lists' which is implemented by the use of lists with acceptable and/or unacceptable URLs²⁰¹.

Appropriate lists or 'White' lists are used to define a domain of 'safe' web sites within which users can browse. These typically require people to search and select sites that are approved by the provider of the list.

Inappropriate lists or 'Black' lists are lists of URLs for which the requests will not be serviced. The list can be compiled by people either working on their own, or as communities of evaluators or by the use of automated machine-executable processes.

Because of the fine granularity provided by this approach, the list of URLs may be very long and thus extremely time-consuming to compose. Especially as all pages within a site must be included in the list to ensure adequate coverage.

Some lists providers use the 'wildcard method' to save time in compiling their lists. When wildcards are used, the lists contain items such as, for instance, 'http://www.inappsite.com/*.*', where the '*.*' allows matching all pages contained within the specified domain.

The weakness of the approach by URLs lists is that the owners of web pages may change their address. And this is particularly the case when those pages contain inappropriate content. The result is a decrease in the efficiency of the lists: the URL changes, but the content is still available somewhere else in the World Wide Web, and will not be filtered out.

Automated text analysis

Another way to analyse information is by using software that scans the text on a site or even the words in a URL to determine the relevance or suitability of the provided information.

The users or groups of users are assigned profiles of interests, in the form of lists of positive and /or negative items; such is the case with white and black lists, that consist of keywords and phrases.

Almost all content based filtering use some variation of keywords matching, where keywords from a profile of interest are compared against the keywords occurring in the content of the specific web page.

Content analysis by comparing phrases is also called profile filtering, which means that keywords are analysed within their context.

Text analysis can be used to screen search terms from search queries, email content, newsgroups, chat sessions, etc as well.

²⁰¹ See also Section 10.2.2 of the September 2002 intermediate report.

*Image analysis*²⁰²

Analysing the content of images is a relatively recent approach and is based on new developed techniques such as the detection of skin tones or on the analysis of the images themselves.

Like profile filtering, image analysis is often used in combination with URL filtering in order to classify sites that are not yet on existing lists.

The following example of using image analysis technology is not in the line of preventive technological devices considered in our study, but is worth mentioning regarding the subject of this report.

- **Swedish National Crime Investigation Department uses ‘Excalibur’**

Today the Swedish National Crime Investigation Department uses Excalibur Technologies’ Visual Retrieval Ware Software²⁰³ in combination with their own database containing known child pornography photos and video films to help in their investigation on paedophiles. The software is able to scan in pictures from CD-Rom, and then search its entire database.

Excalibur’s software is able to recognise the degree of similarity between a searched and a programmed variable with different degrees of information, based on their colour, shape and texture and allows users to ask simple questions like ‘Have you seen anything that resembles this?’ and ‘Where did it originate?’.

The terms of reference for searching do not include the identification of the victims involved, but focus on the background information available i.e. similar colours and textures of walls, carpets and bedding, style, colour and shape of bedstead and number of windows similar level of lighting etc.

- Another example of image analysis technology showed, by using morphological analysis of several children on different paedophile pictures, that the same children were in fact ‘used and abused’ by paedophile networks for several years. This example proves that technologies exist and are useful in the fight against child pornography on the Internet, even though they are not, strictly speaking, preventive.

Packet analysis

Besides the types presented above, another control possibility is through packet filtering.

The content of web pages travels through the Internet in packets of information. Each of these packets contains the IP address of where it is going to, as well as the IP address of where it comes from.

Analysing a packet involves examining the IP address of where the content has come from. If a machine has been identified as spreading illicit content, packet analysis enables blocking that spreading.

²⁰² See Advanced Techniques for Automatic Web Filtering – James Z. Wang

www-db.stanford.edu/pub/gio/slides/WIPE-NRC.ppt

²⁰³ For more information: <http://www.excalib.com> and the Swedish National Criminal Investigation Dept. (childabuse@rkp.police.se).

Packet analysis takes place on a router, because routers steer packets through the Internet from source to destination.

Access authorisation

Software technologies and hardware devices are used to authenticate that a user has the authorization to access given services or data.

This approach allows the further option to make use of age verification technologies (or AVTs), which seek to differentiate between adults and children in an online environment. Age verification is not always simple and cannot always be trusted as will be explained in Section 2.2.3.7.

Encryption, password protection, and credit card validation techniques are types of software technologies that can be applied for authorisation purposes.

Furthermore new biometric algorithms and hardware devices are being developed nowadays, that uniquely identify users using, for example, smartcards, finger scanning, retina scanning, voice print, and the user's individual typing rhythm.

Activity tracing

Internet usage can be traced by using the server log files and other data logs. These files store details of all web accesses and can be configured to analyse web-related activities.

At home this type of technology can be used to trace the Internet activities of children for example. Many monitoring options can be provided, e.g. recording a history of web pages accessed, even keystrokes can be captured in log files, screen capture, etc.

But one has to keep in mind that being controlled can be positive but can have negative effects as well. While it is certainly educational to show to the child what is 'right' for

him/her when exploring the Internet, the child may revolt against his/her parents because they limit and interfere with his/her privacy. A good communication is particularly important so that the children understand that the Internet may really be dangerous for them; and that there are good reasons why the parents wish to exert a certain degree of control on 'where' their children go.

Quality of filtering

Are unwanted sites correctly blocked and do innocuous sites pass through? Do the packages filter out innocent, maybe even educational (or preventive) material whose name can provide confusion, due to the ambiguities in language?

Quality of filtering of the software package (for each different category or also addressed as 'over-blocking' and 'leakage') is not an easy-to-evaluate indicator. For instance, most packages filter pornography very well and other categories (particularly weapons) not so well; the reason is that most packages are American products and they are stricter on pornography material and much more tolerant on weapons.

No technique for Internet content control is infallible and one has to keep in mind that reaching 100% accuracy is not simple, and most likely even unfeasible.

Management of information control

It is not easy to give a clear and objective definition of what is 'inappropriate' and it may even be impossible to do because the level of inappropriateness is different for each individual as they differ in religion, age, etc.

Moreover (young) children cannot always manage and decide themselves on what they think is inappropriate and sometimes they even cannot verify if what they believe is inappropriate is also controlled.

Therefore it is first necessary that parents (supervisors) have the possibility to (pre-) configure different types of user profiles.

Thus additionally it is important to consider

- Who does the classification of web contents
- How the categorisation is made
- Which blocking methods are implemented

These three aspects are dealt with in the following subsections.

Classification

Regardless of what actions are taken, mechanisms are needed to label content or identify content of a particular type. For any system of labelling or classifying content, it is important to understand who (or what kind of automated tool) is performing the classification, and which criteria are used to perform the classification.

Classification may be done by:

- **Content providers.** The Internet Content Rating Association (ICRA) and SafeSurf are examples of PICS rating systems that are designed to be used by content providers.
- **Third-party experts.** Many filtering companies use teams of information specialists, parents, and teachers to assist in classifying contents.
- **Local administrators.** A parent, teacher or other local 'administrator' may personally decide which contents should be accessible to children under his or her supervision.
- **Survey or vote.** Another way to classify Internet content is through a survey or vote. This technique has been used by several organisations to rate restaurants and movies. Recently, Net Shepherd began using this approach with their World Opinion Rating Service. Net Shepherd has established a 'Rating Community' of people who rate and classify contents.
- **Automated tools.** Some companies have developed automated tools to assist in classifying online content. Some of these tools are used to classify content dynamically, as the user requests it. Others are used to assist human classifiers in finding suspect sites.

In relation to this, the company can encrypt the available lists or can offer the user the option to locally review and/or modify the criteria for determining inappropriateness, such as:

- the list of keywords and phrases,
- the list of URL's,

- the company's other criteria for determination.

Moreover when determination criteria, such as lists or categories, are provided by the company, it is necessary that updates are done on a regularly basis. Some products and services are continuously updated and include mechanisms for the user to easily and quickly take advantages of the updates. Others require the user to manually download new updates.

Categorization of information

Using labels for rating Web content, a series of categories and subcategories are used.

The content may be classified on the basis of its age suitability, on the basis of specific characteristics or elements of the content, etc.

When classifying on the basis of characteristics of the content, each category describes the nature of the content such as 'Race', 'Sexual content' or 'Privacy'. Within these categories further specifications can be made such as 'Romance, no sex', 'Partial nudity', etc.

Blocking methods

Different methods can be used to let the user know that the information is inappropriate.

Sometimes the user can specify whether inappropriate content should trigger a block, a warning message, a log entry, or another action.

Blocking information can be implemented by a method called 'x-ing out', which means that the illicit keywords are substituted by 'xxx'.

Another method is 'blocking the entire page or domain' and informing the user by using denial pages where messages such as 'Blocked by <Name of the tool used>' are shown. Some vendors show in their message the reason why the information is blocked and even sometimes provide a feature, which offers the users the possibility to configure themselves the pages and the messages shown.

Configuration and user-friendliness

For a large part of the devices, a certain degree of configuration is required by the user. It may be by setting up profiles for different members of the family, or creating accounts with an ISP for each family member, or customizing a control list.

A point to consider is thus for example to verify if an out of the box-working version is available and if not, what is the type of configuration requested?

Another criterion is the ease-of-installation. Some devices are provided on CD-ROMs, while others are downloadable over the Internet. ISP-based products may or may not require the installation of specific end-user software.

Furthermore, it is important that once the device has been set up, it is easy to use. This means among others straightforwardness to change from one user profile to another, easy to over-ride, and so forth.

Since it is not unlikely that all these tasks will be carried out by a person who may not be technologically literate, the degree of ease with which this can be done is an important parameter.

Security

Each software package needs at least some kind of protection such as passwords enabling. Unfortunately, this kind of protection is not always secure enough. For example, the Internet provides a variety of information on how to hack protective technological devices.

Beside this, the criterion is not only about security as protection from criminal actions, but also about the protection options provided for the user to secure the administration area from unauthorised tampering, meaning from access of technologically literate children that want to bypass or disable the control for example.

System requirements

System requirements describe the type of computer environment (e.g. the platform) that is essential to run the software.

In the case of user-based devices this is especially important, since many home and school users may not have up-to-date computing equipment.

Another aspect is the compatibility of protective devices with other software. The protective device must not prevent another product from working and vice-versa.

Support

A significant feature, which is easily forgotten, is the level of support and the possibilities for feedback that are available.

Especially for private users it is important to have a point of contact in case of a problem.

Examples of such support features available are:

- A telephone number provided to contact a hotline;
- A home site where questions can be posed;
- An email button that is easy-to-see placed in the application.

The level of support may be further characterised by:

- Helpdesk opening hours (round the clock service versus typical business hours)
- The languages in which the assistance is provided (English only versus several other languages)
- Kind of support provided (assistance at home versus via e-mail plus telephone only)

Financial costs

Because the financial cost of a solution may be prohibitive for certain parties or individuals, it constitutes a factor that may impact the efficiency of an approach in the sense that it would not be implemented for financial reasons.

This is particularly important for products addressed to individuals. They should know exactly what they want and the associated cost of the entire individualised package that they buy.

In certain cases, it is possible that each month or each year a certain amount of licence costs need to be paid. Possibly even extra costs may be required like for support or update as new sites are published continuously.

For applications installed at server level, additional costs per computer connected or per users can be asked. Some ISPs may even have arrangements in place whereby they provide control software at reduced (even zero) costs to their customers.

Future

What is the future of the devices and of the technological world today?

Some technologies whose effectiveness is limited today may increase in effectiveness tomorrow as research progresses. Or, some devices may need a certain technology, which already exists and is planned, but not implemented yet.

On the other hand, as the technology changes and ameliorates constantly not only better solutions will rise, as new technologies will then 'enlarge' the pornography problems to fight against and new types of solutions as well.

10.8 HOW TO USE THE INDICATORS: THE RESPECTIVE PROS AND CONS

All control devices have to strike a balance between effectiveness, resource usage and their impact on Internet access. Typically, the more effective control mechanisms are, the more computing resources, such as processor time and memory, are used.

Client-side ('end-user') control mechanism can afford to use more resources because they are only serving at the client side. These devices can also be more flexible and can allow users to determine their own degree of control.

Any mechanism used to filter traffic at an ISP (server-side mechanism) has to be highly efficient in order to be able to handle the volume of requests generated by thousands of concurrent users.

This chapter gives an overview of the advantages and drawbacks²⁰⁴ of each indicator described in the previous chapter.

²⁰⁴ The evaluation indicators provided in this chapter was partly composed by using information of:

CSIRO, Commonwealth Scientific & Industrial Research Organization – Access Prevention Techniques for Internet Content Filtering – Prepared for the National Office for the Information Economy – <http://www.cmis.csiro.au/Reports/filtering.pdf>

Shining a light on Filters in Libraries by Karen G. Schneider MSLIS – <http://www.bluehighways.com/filters/filtersc>

The book 'Youth, pornography, and the Internet' written by Dick Thornburgh and Herbert S. Lin in which dimensions of choice identified by GetNetWise are quoted.

An ethical framework: Mechanisms for user enabled choice and normative claims. http://webworld.unesco.org/infoethics2000/documents/paper_conley.rtf

Location where the protective device is installed

Any Internet content can be controlled either on the end-user's own computer or at their ISP's or both, but not without some inconveniences.

At ISP level

Content control at the ISP's has both advantages and disadvantages when compared to client side control.

The advantages include:

- Ease of installation and use for the end-user,
- More difficult for users (the controlled ones) to bypass or avoid the control features placed on their servers.
- The disadvantages include:
 - Performance impacts including increased delays of reaction and reduced capacity of the overall system,
 - Costs of installing and administering suitable control systems,
 - Potential impact on all Internet users, also the users (adults) that do not want to be controlled (They can experience problems finding the information they want and even encounter delays in their searches for example).

In fact any delays of access restrictions imposed by ISP control mechanisms can have an impact on all Internet traffic, on business as on educational web browsing.

At Client-side level

Client-side ('end-user') control devices can be more flexible and can allow the users to determine their own degree of control.

The impact of client-side filtering is limited to the users themselves and to people under their supervision.

As client-side products only have to deal with requests from one user at a time and a 0.1s delay in displaying a web page would not be noticed at all, performance is not a concern for client-side control.

Architectural choice for ISP located protective devices

The different types of technology that high volume ISPs could use for filtering, all present some advantages and disadvantages as well.

Conventional proxy servers

This is in the first place a performance improvement approach provided by the use of caching. With proxy servers, copies of web contents are kept so that future requests for the same contents can be answered with fetching the pages from the cache rather than having to be fetch again from the Internet.

It is a flexible solution as well because general-purpose computer software and hardware can be used and can be easily adapted to the ISPs filtering needs.

Using conventional proxies, servers can be configured to filter only selected Internet services and thus add no overhead to other services.

On the other hand this technology presents some inconveniences as well.

It requires that clients' web browsers be specially configured. Therefore the ISPs have to contact every client and request that they change their browser configuration. As a consequence, they also have to handle the support calls from those users who are unable to make the required changes, or who just ignored the request and found that they had then lost their Internet access altogether. These actions are very complex and costly.

Additionally, a crash occurring at the proxy level will block all access to the web for users of the proxy until it is repaired or replaced.

Transparent proxy servers

This type of proxies avoids the complexity and costs of the necessity to configure web browsers if proxy servers are not already being used.

It is a flexible solution as well, it can run on standard computer software and hardware too, and can be easily adapted to the ISPs filtering requirements.

This technology however adds some overhead to all Internet traffic and thus may have a negative effect on new time-sensitive services such as 'voice over IP' and streaming media.

Additionally this means that failure of the proxy would block the access to all Internet access for everyone.

Specialised cache engines

These specialised transparent caches are built on communication industry standards and offer high reliability, availability and fault tolerance.

Moreover they offer the best performance but on the other hand also the highest costs because they use custom-designed hardware and software.

They are also able to offer good scalability in handling the caching and filtering needs of large ISPs, through the use of a number of caching engines fed by high performance switches.

It is the least flexible solution however, as specialised hardware and software are needed and as it may not be able to change the built-in filtering mechanisms or support large filter lists.

But temporarily bypassing the cache engines and thus providing unfiltered access instead of no access at all can easily handle a possible failure (a crash for example) of the specialised cache engines.

Foreword about the international dimension

One aspect, which is present for all control mechanism on Internet content, is the international dimension. In fact: 'Data banned in one place may not be banned in others!'

This international nature of the Internet additionally increases the difficulty of distinguishing what may be considered appropriate and inappropriate to the public

Another problem related to the international dimension is the multilingualism.

Blocking pornographic web content based on their associated English keywords may not work well for Dutch, French, Spanish, Russian or Japanese websites, but these non-English pornographic sites can also be found by using search engines.

Furthermore the law differs from country to country. The age of consent, meaning, the definition of what is a 'child', and the laws on privacy as well, may vary considerably from one country to another.

Site Labels or rating systems

Site labelling systems are the most flexible and perhaps hold the most promises for the future.

As already mentioned, labels may be generated by the content provider, third party rating services, communities of users, or individual users. The software installed at the ISP and/or the client level then uses the labels that have been assigned.

As there exist many rating authorities, and different communities may consider the same content to be in different categories, problems may appear.

Questions arise as to the completeness of label coverage in a billion-page web domain and the quality of labels, e.g., as for who generates them and who guarantees them.

Another problem, which can be solved, however is the lack of flexibility in the label categories used nowadays. A more detailed categorisation system is required in order to rate a wider range of materials.

Moreover some people believe that rating that is not carried out by the individual users themselves is just a 'modern face of censorship'. They object that people just do not have the freedom to make up their own minds.²⁰⁵

Lists of URLs

The technology of using lists of URLs can be put in practice by using lists of appropriate or inappropriate sites, also called white and black lists, which is a very fast and simple approach.

White lists

This type of control can be 100% effective; assuming the person or organisation that has compiled the white list shares the same set of values as the Internet user.

Creating a global white list is not possible because people all over the world vary in culture and thus have different ideas of what is inappropriate, and differences of laws on the subject exist as well.

The main drawback of white lists is certainly the fact that they must be long, because of the amount of content available on the Internet. And since there are many more 'good' sites than 'bad' sites, white lists will be bigger than black lists.

On the other hand, the use of white lists is particularly useful to create a child-friendly web environment.

²⁰⁵ Governance of Pornography and Child Pornography – <http://www.cyberrights.org/reports/governan.htm>

Black lists

Black lists are more commonly used than white lists and have the advantage that they are shorter than white lists.

But the main problem with black lists is that they will never be complete as the Internet is enormous. For a black list to be effective, every URL (every page in a site) to be blocked has to be explicitly included in the list and thus building and maintaining these lists is very work intensive. Besides, a large amount of memory has to be allocated to store these lists.

One solution can be adding only the URLs of the domains of the inappropriate sites on the list by using wildcards in the URLs. Using this partly matching technique, the lists are smaller and less memory is used than with exact URL matching. However innocent pages of sites may be easily blocked using this technique.

Another way to avoid the problem of exact URL matching is to use the pattern matching technique on URLs. This technique analyses the words in the URL and thus URLs containing the keyword sex will be blocked for example. This approach however is very prone to error as URLs such as www.middlesex.org.uk will be blocked as well. Additionally as the list with rules grows larger, severe performance problems may appear when the technology is used on ISP level, because every outgoing URL has to be checked against each indicated rule.

Automated text analysis

Keyword filtering

The advantage of keyword filtering is that it adds very little computational overhead, and hence can be implemented on older style personal computers. It is one of the cheapest and simplest technologies for content control.

However it is indiscriminative, as the context is normally not taken into account. The classic example is the term breast cancer, which would be picked up by a keyword filter containing the word breast, resulting in blocking the entire site.

Another problem appears when blacklisted words are contained inside other words for instance a keyword filter with sex in its black list may block documents containing the word Middlesex. This results in legitimate, educational material being blocked.

Keyword Filters are easy to mislead. Some examples of sneaking past filters are:

- Misspelling words: e.g. sex (sez) and pornography (pormography)
- Substituting numbers for letters and letters for numbers is an increasingly common practice: e.g. L0lita
- When the music file sharing peer-to-peer network Napster was ordered to block the access it provided to copyright music, some users began renaming titles in a form of encrypted language to confuse the filter.

Profile filtering

For real time profile filtering, a fair amount of content needs to be fetched from its source before enough analysis can be carried out to determine whether it can be

classified or not. During this time the page, or a good part of it, will have been displayed on the user's screen.

Introducing some understanding of the context and word usage may stop some of the more obvious errors of keyword filtering. Recognising the meaning and nature of written text remains a difficult research problem however.

*Image analysis*²⁰⁶

Effective filtering based on image analysis is feasible with the current technology, but the technology can still – and has to – be improved through further research.

Efforts have been made to characterise images based on the amount of 'flesh tone' in the images and on the poses struck by the subjects in it, but there are still some challenges that have to be worked out: non-uniform image background, textual noise in foreground, wide range of image quality, wide range of camera position, wide range of compositions, video and other streaming media are only some of them. Computers have difficulty distinguishing between fine art and pornography for example.

The image analysis approach is affected by the same issue as profile analysis in the sense that an image or a percentage of it, needs to be loaded before it can be analysed, and during that 'analysis time', it may be displayed on a user's screen. Image analysis is thus very time-consuming as well.

However, knowing that inappropriate websites will contain many objectionable images, these sites are easily identifiable (without having to analyse their pictures each time). So, combining different technologies such as URL filtering, profile analysis and image analysis may attain a good accuracy and acceptable speed. Some products do already filter on the basis of web page structure as well as keywords and images for example.

Statistical profiles of 'pornographic' pages can thus be made, looking at features such as the ratio of text to images, the presence of keywords and 'flesh tones' within images.

Packet analysis

Although the most sophisticated routers can implement packet analysis without performance degradation, the main problem is the efficiency. An IP address represents a particular computer and attempting to filter an Internet site by using its IP number may also block a large number of legitimate sites hosted on the same computer. Therefore packet analysis is not widely used.

Access authorisation

This approach can be very effective as a reverse filter restricts who can have access to a given site, yet many problems, technical and non-technical, remain.

Encryption schemes, such as Public Key Infrastructure (PKI) or Private Key Algorithms require the user to be in possession of a valid key in order for the decryption to occur.

²⁰⁶ Advanced Techniques for Automatic Web Filtering – James Z. Wang

www-db.stanford.edu/pub/gio/slides/WIPE-NRC.ppt

Users wishing to access data or transfer data sites with user ids and passwords must first obtain and keep them. The use of credit cards or proof of age cards over the Internet is the most problematic in terms of guarantee that the user is the right one.

Moreover all these new biometric algorithms and hardware devices available such as smartcards, finger scanning, retina scanning, voiceprint, and user's individual typing rhythm are not all technically mature yet and are expensive as well.

Activity tracing

This approach monitors which activities have been done, rather than actually filtering.

Here privacy issues must be addressed as well, because of the negative effect the monitoring can have on people being monitored.

Especially children may react in a reversed way on monitoring. Monitoring can have the same effects to children as reading their diaries and they can as a result of this, act in a contrary way and start doing what has been told to them not to do. The act of monitoring can therefore be educational or destructive.

Supervisors must therefore react in an instructive way to the inappropriate behaviour to provide opportunities for the child to learn how to make good decisions about Internet use.

The future

The future will bring both better solutions and enlargement of the problem of child pornography on the Internet.

There are two things to keep in mind:

- those who produce and consume sexual content over the years have stayed on the leading edge of new technologies too, and whatever the technological future is like in detail, sexual content will stay excessively present in the initial stages of adoption of any new technology as well.
- because technology changes rapidly, **no final technological solutions will be possible.**

10.9 INDICATOR RELEVANCE ACCORDING TO LOCATION OF CONTROL

The Internet content can be controlled either on the end-user's own computer or at their ISP or both. The relevance of using the indicators described above varies according to the location (ISP or end-user) where the products have focus on.

For this reason the selection criteria for choosing a protective device are different if the device has to be installed at the ISP's or at the end-user's personal computer.

Tables 1 and 2 presents the indicators relevance according to the location of the protective device, together with a short explanation. A plus sign indicates that the indicator is relevant; a minus sign indicates that it is not relevant.

Table 1 Relevance of indicators for control devices located at ISP level

Control device located at ISP level			
Indicator	Relevance	Short explanation	
Scope	+	It is important for an ISP to be able to provide as many protocols (HTTP, FTP, email, etc.) as possible. Both incoming and outgoing communications need to be controllable.	
Architectural choice for placing the control device	+	The right choice of type of server technology is crucial for an ISP in order to comply with the services provided to the customers. The best choice is of course the use of "specialised cache engines" but it is an expensive technology.	
Type of technology	+	On top of the above, control technologies need to be added. Here performance has to be kept in mind. Therefore ISPs best use a priori technologies such as "Site labels or rating", "Lists of URLs" and "Keyword filtering".	
Quality of filtering	+	The quality is especially relevant at this level. As ISPs have clients, who differ in various points (culture, age...), it is important that everyone receives "their" appropriate information and have "their" inappropriate ones blocked.	
Information control management	Configuration of user-profiles	+	ISPs especially need to have the ability to specify which degree of control they want applied to the different groups of users they target.
	Who does the classification	+	The classification method used determines the subjectivity degree and the quality of control. Thus in addition to automated-machine classification, human verification is indispensable.
	Review/Modification of criteria of inappropriateness	+	ISPs are required to provide their customers with the ability to review the criteria of inappropriateness and possibly adapt them to their personal wishes.
	Updates Management	+	The criteria of inappropriateness always have to be as up-to-date as possible.
	Categorisation	+	Categorisation needs to be complete and tuned to comply with the differences of people.
Blocking methods	+	ISP Customers must be properly informed by clear messages on the reasons why certain content is blocked.	
Configuration and user-friendliness	-	This is less important for ISPs as they have the technological skills needed.	
Security	+	Security is in fact essential, but can also be provided by other means than the control software used at ISP level.	
System requirements	-	Less important for ISPs as they usually have the system requirements needed.	
Support for administrators	-	Less important for ISPs as they have the technological skills needed.	
Price	-	The price consists of two parts for ISPs: The costs of procurement for the ISP itself.	
	+	The costs charged to the customers for the use of the ISPs services.	

Table 2 Relevance of indicators for protective devices located at end-user's level

Control device located at End-user level			
Indicator	Value	Short explanation	
Scope	+	The scope of the product depends on the wishes of the end-user.	
Placement of controlling	0	Not applicable	
Type of technology	-	For end-user this is less important as they do not have the same concern on the level of performance as the ISPs.	
Quality of filtering	+	At home the computer is used as a learning tool as well as an entertainment tool. Therefore it is important that the tool doesn't over-block and under-block for home-individual needs.	
Information control management	Configuration of user-profiles	+	For end-users that want to control the activities of children with in different age groups this is important. It needs to be easy to do.
	Who does the classification	+	The tool / person that does the classification determines the subjectivity and the quality of control.
	Review/Modification of criteria of inappropriateness	+	Also for end-user it is important to be able to review the criteria of inappropriateness and possibly adapt them to their personal wishes.
	Updates Management	+	The criteria of inappropriateness have to be as up-to-date as possible. For the end-user it needs to be easy to do the update.
	Categorisation	+	Categorisation needs to be complete and fine-grained to comply with the differences of each individual.
	Blocking methods	+	The children must be properly informed of the reasons why certain information is blocked. It can provide opportunities for the child to learn how to make good decisions about Internet use.
Configuration and user-friendliness	+	Very important as they do not always have the technological skills needed.	
Security	+	It is especially important for end-users that children cannot easily tamper the product.	
System requirements	+	People at home may not be obligated to buy expensive extra devices in order to let the control device work.	
Support for administrators	+	As end-users may not be gifted with the necessary technical skills, support needs to be available to their needs and as clear as possible	
Price	+	The costs of procurement have to comply with the quality of the product. And also charges (like updates or support) need to be clear to the end-user as well.	

10.10 OVERVIEW OF EXISTING PRODUCTS

There is a great choice of products on the market today. Unisys has selected 58 among the most known manufacturers active in the domain of protective devices and we have tried to draw a kind of specifications sheet for each product, using the indicators presented in this report.

With this aim in mind we sent a questionnaire to the 56 manufacturing companies at the end of October 2003 asking them to return it by mid-November 2003. 13 companies responded to the questionnaire. For the products for which we did not receive the completed questionnaire, we gathered as much information as possible via the manufacturer's website.

The resulting specifications sheets (i.e. the filled-in questionnaires) are provided in Appendix 1. The products are alphabetically ordered (no evaluation is made). To indicate which questionnaires were completed by Unisys, we added **Unisys** to their header.

The subsections below present synthetic views of the information gathered via the questionnaires.

Overview of products according to type and location of the protective device

Table 3 presents an overview of the different products providing information about type and the location where they can be installed. The products are alphabetically listed.

Product	Company	Product type							Control location		
		Special Browser	Search engine / portal	Proxy application	ISP application	Restricted access app.	Filter (PC application)	Other	End user	Server or ISP	ISP + user
Access Management Engine Activity Monitor	Bascom TrueActive Software				X		X		X	X	X
AOL Parental Controls Bounce	AOL One Light Corporation	X				X	X		X	X	X
BrowserLock Bsecure	Dragon Enterprises Bsafe Online						X	X	X		
ChiBrow ChildSafe	PeopleNet International WebRoot Software 711.Net	X				X		X	X		
Cleanweb Filtering Services				X				X	X	X	
ComputerCop Deluxe							X		X		
ContentKeeper Web Filtering				X				X		X	
Contexion	RuleSpace Inc.	X	X	X	X	X	X		X	X	X
Cyber Sentinel	Finer Technologies Inc.						X		X		
Cyber Snoop	Pearl Software Inc.						X	X	X	X	
CyberPatrol CyberSitter	Surfcontrol Inc. Solid Oak Software Inc.						X		X	X	
dSPAM ENUFF eTrust Intrusion Detection	Dragon Enterprises Akrontech Computer Associates				X	X		X	X		X
FilterPak	S4F							X	X		
Firetrust MailWasher Freedom Parental Control	Firetrust Zeroknowledge					X		X	X	X	
IF-2003	Turner and Sons Production Inc.				X					X	
I-Gear	Symantec Corporation				X					X	
Internet Sheriff	Tel.Net Media			X	X					X	
iWayPatrol	iTech Inc.			X					X		
KidSafe Explorer KidsNet	Arlington Software Kidsnet, Inc.	X					X		X	X	

Product	Company	Product type						Control location		
		Special Browser	Search engine / portal	Proxy application	ISP application	Restricted access app.	Filter (PC application)	Other	End user	Server or ISP
Line-Loc							X	X		
Mailwasher Maranatha Filter	Mailwasher			X	X		X	X	X	
MoM	A. Value Systems						X	X		
N2H2	Secure Computing				X				X	
Net Guardian	Maximum Internet Limited			X	X				X	
Netfilter	nXp Technologies			X	X				X	
NetIQ Webmarshal	Ancoris Limited			X	X				X	
NetNanny	Bionet Systems	X						X		
Netprotector	The Modern Lock Company						X	X		
Norton Internet Security	Symantec Corporation					X	X	X		
Optenet	Optenet			X	X			X	X	
Perkeo++	Autem GmbH						X	X	X	
PureSight	iCognito					X		X	X	X
R3000	8e6 Technologies						X		X	X
SentryCam							X	X		
SmartFilter	Secure Computing			X	X				X	
The SpamCop Email System	SpamCop			X		X	X		X	
SurfControl Total Filtering Solution	SurfControl Inc.			X	X				X	
The Bair	Xexotrope				X	X				X
Too COOL	Software 2010	X						X		
WatchDog				X	X	X	X	X	X	
WebDoubler	Maxum Development Corp.			X	X				X	
We-Blocker WebSence				X	X		X	X	X	
WiseChoice Internet Filtering	WiseChoice			X						X

Table 3 Overview of product type and control location per product

Overview of products for ISP-located protection according to technological approach

Table 4 provides an overview of the products that can be installed on ISPs, categorised according to the technologies that the collected ISP products are based on. The products are alphabetically listed.

Product	Technology											
	Conventional proxy servers	Transparent proxy servers	Specialised cache engines	Site labels / Ratings	URL White lists	URL black lists	Text analysis	Profile filtering	Image analysis	Packet analysis	Access authorisation	Activity tracing
Access Management Engine	X				X	X						
AOL Parental Controls	X			X	X	X						
Cleanweb Filtering	X				X		X	X				
Services ContentKeeper Web Filtering					X	X	X	X			X	
Contexion				X	X	X		X			X	
Cyber Snoop eTrust Intrusion Detection				X	X	X	X	X		X	X	X
IF-2003	X				X			X				X
I-Gear								X				X
Internet Sheriff	X			X	X	X	X	X	X			
iWayPatrol				X	X	X	X	X			X	
Kidz.Net		X			X	X				X	X	
Maranatha Filter	X				X	X	X	X				
N2H2					X	X	X	X			X	
Net Guardian	X			X		X						
Netfilter	X					X	X	X				
NetIQ Webmarshal	X				X	X	X	X			X	X
Optenet	X				X	X	X	X				
Perkeo++												
PureSight												
R3000					X	X	X	X		X		
SmartFilter	X				X	X						
The SpamCop Email System	X											
SurfControl Total Filtering Solution	X				X	X	X	X	X			
The Bair					X	X						
WatchDog	X											
WebDoubler	X			X	X	X	X	X				
WebSense	X				X	X						
WiseChoice Internet Filtering		X				X	X					

Table 4 Overview of technologies implemented by available products for ISP-located devices

Overview of products for End-user located protection according to technological approach

Table 5 provides an overview of the products that can be installed on end-user's computers, categorised according to the technologies that the collected end-user's products are based on. The products are alphabetically listed.

Product	Technology								
	Site labels / Ratings	URL White lists	URL black lists	Text analysis	Profile filtering	Image analysis	Packet analysis	Access authorisation	Activity tracing
Activity Monitor									
Bounce		X	X		X				
BrowserLock		X	X						
Bsecure		X	X	X	X		X	X	X
ChiBrow		X	X		X				
ChildSafe		X	X	X	X				
ComputerCop Deluxe					X				
Cyber Sentinel					X				
CyberPatrol		X	X	X	X		X	X	
CyberSitter	X	X	X	X	X				
dSPAM					X				
ENUFF									X
FilterPak		X	X	X					
Firetrust MailWasher								X	
Freedom Parental Control									
KidSafe Explorer		X	X						
KidsNet	X	X	X						
KidWeb		X	X	X					
Line-Loc									
Mailwasher		X	X						
MoM		X	X	X	X				X
NetNanny		X	X	X	X				
Netprotector									
Norton Internet Security		X	X	X	X				
SentryCam									
Too COOL									
We-Blocker		X	X	X					

Table 5 the technologies the end-user products evaluated are based on end users' computer

10.11 CONCLUSION

The Internet is not a child-friendly environment at all, as children may be exposed at various levels to inappropriate Internet material or experiences through a variety of channels, such as Web pages, e-mail, chat rooms, instant messages, Usenet newsgroups, and peer-to-peer file-sharing connections. Children have to be protected as they are sometimes too confident and too young to understand what is appropriate for them and what is not. Hopefully, many preventive technological devices already exist and are developed nowadays.

However, emphasis must be put on the fact that none of the technologies is 100% effective and that the content of the Internet is, by its very nature, anonymous and volatile. Also, as each individual is different and as the technologies on which the control mechanisms present majors differences as well, there is no perfect solution. So choosing the right device depends on various factors and the indicators provided in the present report may help making the right decision.

Nonetheless one has to be aware of the following important facts:

- The Internet is not static, nor is the World Wide Web. New pages are being added to the web at the rate of hundreds of millions every year and just building and maintaining effective filter lists is an immense undertaking. New sites and pages appear every minute and any group or company attempting to prepare comprehensive and complete criteria (filtering, categorisation) lists will always be running behind.
- The criteria lists will never be complete and satisfying because they need to be flexible and adjustable to individual wishes, but cannot, on the other hand be tailored for each individual (as people differ in age, culture, religion, etc.).
- The used technologies are sometimes incapable of distinguishing between information sense and intention (e.g. a sexual solicitation sent by e-mail and a news story about restrictions on online pornography or between a computer virus and a story about a computer virus); this implies that users cannot be sure that content will be rated appropriately and that perfectly innocuous content will not be blocked.
- Systems are easily misled by the use of substitution letters, etc.
- Furthermore, using real-time types of filtering approaches can considerably slowdown the system performance. Therefore those filtering techniques based on dynamic examination content coming from the Internet are suitable for client side use only. (From a performance level of expectations point of view, ISP-based control mechanism has to handle thousands of requests per second, so even simple keyword matching would have trouble operating at this rate. And more complex mechanisms, such as those based on context and image analysis, would simply be impractical.

In order to increase efficiency, technologies have to be used in combination and in layers, and both at the ISP and the end-user level, as for instance, a combination of labels and URL lists used at the ISP in conjunction with a final filter at the client level using local lists and/or automated analysis techniques.

In addition to the above, further development of technological devices, extra regulations and the creation of standards are and will remain necessary in order to continuously improve the protection of children against child pornography material.

The technology partners do not necessarily have to evolve just 'for the sake of technology'. It would be profitable to everyone if technology providers adopted an holistic approach regarding the fight against child pornography, as well as regarding other related types of crimes. They could broaden their actions towards other aspects than purely technological, and towards the other actors in the field of fighting against child pornography

They could pay more attention to the problematic of computer literacy, as ignorance of the user increases his/her risk of being (or having his/her child) victim of child pornography, and more globally, as it may lead to a two-speeds society.

For instance, technology providers

- could define (analyse, standardise, automatise) working procedures in order to optimise specific and/or overall collaboration between them (ISPs, hotline managers, device/tool producers) and the other partners;
- could promote or improve communication channels with the other partners (eg. working seminars with the police or legislative representatives , discussion forum with research centres, informative website, ...);
- they could be proactive in terms of information, especially towards end-users and children, by initiating clear and adapted messages popping up on the end-user's screen each time they launch the Internet, for instance;
- they could be included, or at least consulted, in the conception of educative programs for both adults and children (at school), underlining what could be the dangers of the Internet; describing how to use it safely and what are its possibilities, helping everyone to understand each one's responsibilities.

These are only a few suggestions on how technology providers may contribute to the development of a common sense preventive attitude towards the Internet, much like adults very naturally instil children not to accept sweets and not to follow unknown persons.

11. RECOMMENDATIONS

This section contains a series of recommendations intended to provide the EU Commission and the key stakeholders in the field of child pornography on the Internet prevention with suggestions in order to improve the effectiveness of the measure in place in EU Member States to tackle child pornography on the Internet.

The recommendations are divided into sections reflecting the research path: the first two recommendations are general in the sense that it is possible to address them to the different key stakeholders in the different Areas of intervention.

The other recommendations have been singled out from the research findings and from the seminar proceedings of every single Areas of intervention.

General Recommendations

Recommendation n°1

Background and rationale:

The research findings have highlighted the paucity of data enabling a meaningful evaluation of the preventive measures adopted in the field of child pornography on the Internet. Despite the large amount of information processed and made available by the different key stakeholders dealing with child pornography on the Internet, the data currently available are diverse and far from being comparable.

Recommendation:

Action should be taken at an EU level to promote the development of common standards in data gathering procedures in the different Areas of intervention.

Recommendation n°2

Background and rationale:

From the research findings and in particular from the seminar proceedings, it emerged that people working on tackling child pornography on the Internet suffer negative impacts on their health and safety due to the cruel images and delicate situations they have to look at and deal with every day.

Recommendation:

Action should be taken at an EU level to foster initiatives for continuous psychological support for the workers dealing with child pornography on the Internet. Turnover, for example, in this particular working environment could help reducing the negative impact produced by the child abuse images and by the delicate situations workers have to face daily.

**Recommendations for Area of intervention A
(Area Detection and Control)**

Recommendation n°3

Background and rationale:

Differences in national standards for the collection and usage of digital evidence across EU Member States are a very sensitive problem. It often occurs that the legal procedures for the collection of evidence in a certain EU country are regarded as unlawful in other EU Member States. For this reason, courts in a given Member State may reject the evidence collected in another Member State, thus hampering the successful prosecution of the case.

Recommendation:

Action should be taken at an EU level to further harmonize MS legal and procedural standards related to the collection, validity and use of digital evidence in cases of computer crime and computer related crime. This could be achieved through the creation of a *Law Enforcement Certificate* to be accepted in all the EU Member States. This certificate would officially state the parameters within which the evidence was collected, respecting minimum standards to be set on the basis of Civil Rights and Fundamental Freedoms.

Recommendation n°4

Background and rationale:

From the discussion with experts belonging to the Specialised Law Enforcement Units in the European Union it emerged that prosecutors and judges do not always have the appropriate instruments to correctly understand and interpret computer crime related evidence. This may impair the successful prosecution of a given criminal case.

Recommendation:

Action should be taken at an EU level to provide prosecutors and judges with the necessary knowledge to understand the techniques used for the collection of digital evidence and to correctly interpret it. This could be achieved through the setting up of periodic training seminars.

Recommendation for Area of intervention B (Area Self-regulation)**Recommendation n°5***Background and Rationale:*

From the research findings it is clear that both public and private bodies are aware of the crucial role that self-regulation – codes of conduct particularly – may play in the prevention of child pornography on the Internet. Nevertheless, existing codes of conduct are still heterogeneous and sometimes incoherent with the purpose of controlling and preventing in specific child pornography on the Internet. This can ultimately affect their effectiveness.

Recommendation:

Action should be taken at an EU level to promote the adoption at MS level of a set of minimum standards for effective codes of conduct. It would be useful, for example, to set clear procedures for cooperation with law enforcement agencies, or effective sanctions to act as a strong deterrent.

Recommendation n°6*Background and rationale:*

Notwithstanding the existence of a leading entity such as INHOPE, the European hotline scenario is still highly fragmented. Specifically, the exchange of information between the various hotlines and between hotlines and other key stakeholders in the field of child pornography does not take place on any systematic and routinely organised basis.

Recommendation:

Action should be taken at an EU level to enhance the cooperation, coordination and the exchange of information and data within the hotline network and between hotlines and other key stakeholders.

**Recommendations for Area of intervention C
(Area Awareness and Educational Initiatives)**

Recommendation n°7

Background and rationale:

The research findings highlighted the existence of a large number of actors in the field of awareness and educational initiatives. Unfortunately, it seems that this field suffers from a certain lack of coordination between these actors, which reduces the effectiveness of their efforts to tackle child pornography on the Internet.

Recommendation:

Action should be taken at an EU level to create an EU level organisation acting as an umbrella for the different public and private bodies in the field of awareness and educational campaigns to tackle child pornography on the Internet. In the framework of the initiatives by this organisation it could also be possible to set up a permanent forum for Awareness in which sharing information, exchanging ideas and possibly to set common and EU level strategies to increase the effectiveness of awareness and educational campaigns in EU Member States.

Recommendation n°8

Background and rationale:

As stressed by experts in the field, a need to develop up-to-date awareness campaigns to the fast changing character of the Internet is widely perceived. Specifically, new media such as mobile phones with cameras, are of great concern as they are susceptible to greatly facilitating the production and distribution of pornographic material involving children, and to facilitate communication among paedophiles. Parents and children, as well as the private and public subjects involved in the prevention of child pornography, often lack a complete understanding of these issues.

Recommendation:

The EU Commission should promote the enlargement of the focus of awareness campaigns to include the new media in order to set strategies for effective knowledge-based prevention of the illicit behaviours committed by means of these new technological solutions.

This could be achieved through research projects and educational initiatives aimed to increase knowledge regarding the impact of these instruments on society. It would also be important for the EU Commission to create round tables with all the key stakeholders in the field, such as awareness organisations, NGOs, manufacturers and service providers to act proactively in this field.

**Recommendation for Area of intervention D
(Area Technological Measures)**

Recommendation n°9

Background and rationale:

Even if in this research only the dark side of the Internet emerges, it is important not to demonise this media. The pro-active role that both the Internet new IC technologies can play in tackling child pornography is sometimes underestimated and underused.

Recommendation:

Action should be taken at an EU level to promote the exploitation of the potential offered by the Internet to set strategies in order to increase end-user education regarding child pornography on the Internet and cyber crimes in general. In other words, to consider the Internet as a pro-active instrument for the prevention of on-line child pornography. For this purpose, the EU Commission could encourage the industry and the awareness raising actors to work together in order to improve the technological alphabetisation of Internet end-users.

Recommendation n°10

Background and rationale:

From the research findings and from the discussion with experts in the field, the necessity to create a safer Internet environment clearly emerges. What seems to be most important is the perception of this safer environment for the end-user, starting from the beginning of his/her web surfing and during the whole navigation.

Recommendation:

Action should be taken at an EU level to assess the feasibility of an *EU Safe Site Certificate* to be applied to web sites that are child pornography or child exploitation free, in the sense that they provide completely legal and child oriented material.

The perception of a safe Internet environment is indeed a crucial issue in tackling child pornography on the Internet. An *EU Safe Site Certificate* could be a very pragmatic solution to make the surfer aware that he can trust the virtual place he/she is surfing.

Attention should be paid to set appropriate parameters for this Certificate. It would be advisable to set these parameters after a discussion with the key stakeholders in the field of the prevention child pornography on the Internet and with representatives from Civil Rights Associations in order to avoid any risk of censorship of the Internet content

12.**BIBLIOGRAPHY****MAIN LEGISLATIVE FRAMEWORK**

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet, doc. n. COM (96) 487.

Green Paper on the protection of minors and human dignity in audiovisual and information services, 16 October 1996.

Joint Action of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children, doc. n. 97/154/JHA, published on the Official Journal L 063, 4 March 1997, pp. 2-6.

European Parliament Committee on Civil Liberties and Internal Affairs, Report on the Commission communication on illegal and harmful content on the Internet (COM(96)0487 – C4-0592/96), 20 March 1997, available online at <http://www.saferinternet.org/funding/legislation.asp>. Resolution on the Commission Communication on Illegal and Harmful Content on the Internet, published on the Official Journal No. C 150, 19 May 1997, p. 0038.

Council Recommendation of 24 September 1998 on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, doc. 98/560/EC, published on the Official Journal L 270/48 of 7 October 1998.

Decision n. 276/1999/EC of the European Parliament and of the Council adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, published in the Official Journal L 33, 6 February 1999, pp. 1-11.

Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, published on the Official Journal L 142, 5 June 1999, pp. 1-2.

Communication from the Commission to the Council and the European Parliament, 'Combating trafficking of human beings and combating sexual exploitation of children and child pornography' – Proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography, COM (2000) 854 final/2.

Council Decision of 29 May 2000 to combat child pornography on the Internet, published in the Official Journal L 138, 9 June 2000, p. 1.

Commission of the European Communities, Evaluation report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, COM(2001)106 final.

Council Resolution on the contribution of civil society in finding missing or sexually exploited children, published on the Official Journal C 283, 8 October 2001, p. 1.

Council of Europe Convention on Cybercrime, available online at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>.

Council of Europe Convention on Cybercrime, Explanatory report, available online at <http://conventions.coe.int/Treaty/en/reports/Html/185.htm.htm>

Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, Follow-up to the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, Proposal for a Decision of the European Parliament and of the Council amending Decision No 276/1999/EC adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, doc. n. COM 2002 152, 22 March 2002, available online at <http://www.saferinternet.org/funding/legislation.asp>.

GENERAL BIBLIOGRAPHY

J. Carr, 'Child Pornography', paper presented at the *2nd World Congress against Commercial Sexual Exploitation of Children*, Yokohama, Japan, 17–20 December 2001, available online <http://focalpointngo.org/yokohama/themepapers/theme1.htm>.

Conference of the G8 Ministers of Justice and Interior, *Communiqué*, Milan (Italy), 26–27 February 2001, available online at <http://www.g7.utoronto.ca/g7/adhoc/justice2001.htm>.

Department of Justice, Equality and Law Reform, *Illegal and Harmful se of the Internet*, first report of the working Group, July 1998, available online at <https://www.hotline.ie/html02/reports.htm>.

G8 Justice and Interior Ministers' Meeting, *G8 Recommendations on Transnational Crime*, Part IV, Section D, High-Tech and Computer-Related Crime, 13–14 May 2002 – Mont-Tremblant, Quebec (Canada), available online at <http://www.g8j-i.ca/english/doc1.html>.

K. Koomen, 'Illegal and harmful content on the Internet', paper presented at the conference *Internet Crime*, Melbourne, 16–17 February 1998.

M. Machill, J. Waltermann (eds), *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Germany, 2000.

MAPI, *Child Pornography on the Internet*, report available online at <http://www.info.fundp.ac.be/%7Emapi/mapi-fr.html>.

National Center for Missing and Exploited Children, *1999 Annual Report*, available online at <http://www.missingkids.com>.

UNESCO, 'Declaration and Action Plan', presented at the Expert meeting *Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: an International Challenge*, Paris, 18–19 January 1999, available online at http://mirror-us.unesco.org/webworld/child_screen/conf_index.html.

UNICEF, *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, available online at <http://www.unhchr.ch/html/menu2/dopchild.htm>.

United States Embassy Stockholm, 'Child pornography: an international perspective', paper presented at the *World Congress Against the Commercial Sexual Exploitation of Children*, 27–31 August 1996, available online at http://www.usis.usemb.se/children/csec/child_pornography.html.

AREA OF INTERVENTION A (DETECTION/CONTROL MEASURES):

Y. Akdeniz, *Sex on the Net. The dilemma of policing cyberspace*, Garnet Publishing Limited, United Kingdom, 1999.

Y. Akdeniz, *Regulation of child pornography on the Internet*, May 2002, available online at <http://www.cyber-rights.org/reports/child.htm>.

C.A. Arnaldo, *Child abuse on the Internet. Ending the silence*, UNESCO Publishing, 2001.

J. Carr, 'Child Pornography', theme paper presented at the *2nd World Congress against Commercial Sexual Exploitation of Children*, Yokohama, Japan, 17–20 December 2001, available online <http://focalpointngo.org/yokohama/themepapers/theme1.htm>.

European Union, *Interim report on Initiatives in EU Member States with respect to Combating Illegal and harmful content on the Internet*, 4 June, 1997, available online at <http://europa.eu.int/ISPO/legal/en/internet/wp2en-chap.html#2A>.

Europol, *Manual on child Pornography legislation*, Unit Trafficking in Human Beings, March 2001.

Interpol, *Legislation of Interpol member states on sexual offences against children*, available online at <http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp>.

République Française, *Lutte contre les réseaux incitant à la pédophilie. Protection des mineurs sur internet. La loi*, available online at <https://www.internet-mineurs.gouv.fr/lois.htm>;

Service des Affaires Europeennes, *La lutte contre la pornographie enfantine*, France, May 2001, report available online at http://www.senat.fr/lc/lc90/lc90_mono.html.

U. Sieber, 'Responsibility of Internet Providers - A comparative legal study with recommendations for future legal policy', in *Computer Law & Security Report*, vol. 15, n. 5, 1999.

U. Sieber, 'legal Regulation, law Enforcement and Self-Regulation: A New Alliance for Preenting Illegal Content on the Internet', in *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, 2000, pp. 319–399.

G. Van Bueren, 'Child Sexual Exploitation and the Law. A report on the International Legal Framework and Current National Legislative and Enforcement Responses', theme paper presented at the *2nd World Congress against Commercial Sexual*

Exploitation of Children, Yokohama, Japan, 17–20 December 2001, available online http://focalpointngo.org/yokohama/themepapers/theme_law.htm.

AREA OF INTERVENTION B (SELF-REGULATION):

A) HOTLINES

H. Burkert, 'The Issue of Hotlines', in *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, 2000, pp. 263–318.

ICRI K.U. Leuven, *Legal issues with regard to the activities of hotlines in the battle against child pornography on the Internet*, Belgium, June 2001 (also available online at <http://www.protegeles.com/informes/Deliverable1.pdf>).

INHOPE Association of Internet Hotlines Providers in Europe, *First Report*, INHOPE, May 2002, available online at www.inhope.org.

M. Machill, A. Rewer, *Internet-Hotlines. Evaluation and self-regulation of Internet content*, Verlag Beltersmann Stiftung, Germany, 2001.

N. Williams, *The contribution of Hotlines in Combating Child Pornography on the Internet*, available online at www.childnet-int.org.

B) HOTLINES WEB SITES

Stopleveline, Austria, available online at www.hotline.ispa.at/index_e.html;

Child Focus, Belgium, available online at http://www.childfocus-net-alert.be/uk/UK_childfocus_sub02.htm;

Red Barnet Hotline, Denmark, available online at www.redbarnet.dk;

Save the Children, Finland, available online at <http://www.pela.fi/>;

AFA, France, available online at www.pointdecontact.net;

FSM, Germany, available online at www.fsm.de;

ECO Electronic Commerce Forum, Germany, available online at <http://www.eco.de/servlet/PB/menu/-1/index.html>;

Jugendschutz, Germany, available online at www.jugendschutz.net;

Irish hotline, Ireland, available online at www.hotline.ie;

Meldpunt Kinderporno, Netherlands, available online at www.meldpunt.org;

Protegeles, Spain, available online at www.protegeles.com;

FACE IT, Sweden, available online at www.rb.se/hotline/;

IWF, United Kingdom, available online at <http://www.iwf.org.uk/hotline/>.

C) HOTLINES PERIODIC REPORTS

Stopleveline, Austria, *Annual Report 2001*, available online at <http://www.stopleveline.at/Page-Who-are-we.htm>;

- Red Barnet Hotline, Denmark, *Reports 2001*, available online at www.redbarnet.dk;
- Save the Children, Finland, available online at <http://www.pela.fi/>;
- Irish hotline, Ireland, *First Report. November 1999–June 2001*, available online at www.hotline.ie;
- Meldpunt Kinderporno*, Netherlands, *An evaluation of the Internet Hotline against Child Pornography*, available online at www.meldpunt.org/rapport-eng.html;
- Protegeles*, Spain, *Legal Manual for a Spanish Hotline battling against child pornography on the Internet*, available online at <http://www.protegeles.com/informes/LEGALMANUAL.pdf>;
- FACE IT, Sweden, *statistics 1999–2001*, available online at www.rb.se/hotline/estatistik.htm;
- IWF, United Kingdom, *Internet Watch Foundation Third Annual Report*, available online at www.iwf.org.uk/about/main_annual99.htm.

D) CODES OF CONDUCT

- AFA Association des Fournisseurs d'Accès et de Services Internet, *Standards and practices*, January 1998, available online at <http://www.afa-france.com/html/accueil/mend2.htm>.
- AiIP Associazione Italiana Internet Providers, *Codice di Autoregolamentazione per i servizi Internet*, available online at <http://www.aiip.it/autoreg.html>.
- ASIMELEC, *Código profesional de las empresas proveedoras de servicios de Internet de Asimelec*, available online at <http://www.asimelec.es/>.
- Bertelsmann Stiftung, 'Toward a Model Code of Conduct on the Internet', paper prepared for the conference *Self-Regulation of internet content, Workshop 'Codes of Conduct'*, Hannover, Germany, 30 June 2000, available online at <http://www.stiftung.bertelsmann.de/internetcontent/english/content/c2420.htm>.
- M. Cammarata, A. Monti, *Proposta per un codice di autoregolamentazione dei fornitori di servizi telematici*, 1 April 1997, available online at <http://www.interlex.com/regole/codice.htm>.
- CILPF Internet Law and Policy Forum, *A borderless world: Realizing the potential for global electronic commerce. Observations on the state of self-regulation of the Internet*, prepared for the Ministerial Conference of the Organisation for Economic Cooperation and Development (OECD), Ottawa, Canada, 7–9 October 1998, available online at www.ilpf.org/events/selfreg/.
- Council of Europe, Questionnaire on self-regulation and user protection against illegal or harmful content on the new communication and information services. Summary and analysis, available online at http://www.coe.int/t/e/cyberforum/country_information/Summary_and_analysis/default.asp#TopOfPage.
- A. Gidari, 'Observations on the State of Self-Regulation of the Internet', paper prepared for the Ministerial Conference of The Organisation for Economic Cooperation and Development ('OECD') *A Borderless World: Realizing the Potential for Global Electronic Commerce*, Ottawa, Canada, 7–9 October 1998, available online at <http://www.ilpf.org/events/selfreg/>.
- IAPCODE, *Selfregulation.info*, available online at selfregulation.info;

International Federation for Information Processing, Special Interest Group 'IFIP Framework on Ethics of Computing', *Documents d'autoréglementation – Classification – Un premier inventaire*, September 2000, available online at <http://www.info.fundp.ac.be/~jbl/IFIP/sig922/selfreg.html>.

Internet Resources on Self-Regulation and the Internet, available online at http://www.law.washington.edu/lct/files/95_self_regulation.doc.

Internet Service Providers Association of Ireland, *Code of Practice and Ethics*, available online at <http://www.iab.ie/Publications/Reports/d33.PDF>.

ISPA Austria, *Code of conduct*, available online at <http://www.ispa.at/Richtlinie/Richtlinie.htm>.

ISPA Belgium, *Cooperation protocol in order to combat illegal acts on the Internet*, available online at <http://www.ispa.be/en/c040201.html>.

ISPA United Kingdom, *Code of Practice*, adopted by ISPA on 25 January 1999, available online at http://www.ispa.org.uk/html/body_code_of_practice.htm.

M. Machill, J. Waltermann, 'Memorandum on Self-Regulation of Internet Content', in *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, 2000, pp. 23–57.

OECD Directorate for Science, Technology and Industry, *Proceedings of the OECD/BIAC Forum on Internet Content Self-regulation*, OECD, Paris, 25 March 1998, available online at <http://www1.oecd.org/dsti/it/secur/act/selfreg-links.htm>.

M. Price, S. Verhukst, 'The Concept of Self-Regulation and the Internet', in *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, 2000, pp. 133–198.

AREA OF INTERVENTION C (AWARENESS AND EDUCATIONAL INITIATIVES)

A) GENERAL LITERATURE

Arnaldo, Carlos A. (ed.) (2001), *Child Abuse on the Internet. Ending the Silence*, Paris: UNESCO & Berghahn Books.

Campagna, Norbert (1999), *La pornographie, l'éthique et le droit*, Paris: Harmattan, Paris.

Carr, John (2001), 'Child Pornography', paper delivered to Second World Congress against Commercial Sexual Exploitation of Children, Yokohama, 17–20 December, 2001.

Commission européenne (1999), *Combattre la pornographie enfantine sur Internet*, Editions Conférence internationale de Vienne.

Conseil d'Etat (1998), *Internet et les réseaux numériques*, Paris: La documentation française.

ECPAT (1999 & 2000), 'Five Years after Stockholm. 2000–2001' *The Fifth Report on the Implementation of the Agenda of Action adopted at the First World Congress against Commercial and Sexual Exploitation of Children in Stockholm, Sweden, 28 August 1996*.

- Florence, Bruce (1996), *L'exploitation sexuelle des enfants*, Paris: Fayard.
- Fournier de St Maur, Agnès (1999), *L'exploitation sexuelle des enfants à l'aide d'internet: un nouveau défi pour Interpol*, Paris: UNESCO.
- Guyenot, Laurent (2000), *Le livre noir de l'industrie rose, de la pornographie à la criminalité*, Paris: Imago.
- Jones, Logan M. (1998), 'Regulating child pornography', *International Journal of Children's Rights* (6) 1998
- Kane, June (1998), *Sold for Sex*, Arena.
- Kane, June (1997), *Chasse à l'enfant*, Paris: Ramsay.
- Mutschke, Ralf (1998), *Utilisation d'Internet dans le cadre de l'exploitation sexuelle infantile*, Strasbourg: Conseil de l'Europe.
- Ruxton, Sandy (2001), *Child Sexual Exploitation: An Action Plan for Europe*, Stockholm: Save the Children Alliance.
- Ruxton, Sandy (1996), *Children in Europe, England: NCH Action for Children*.
- Sieber, Ulrich (1999), *Criminal law provision against child pornography: a legal comparative study for the creation of worldwide minimum standards*, University of Wurzburg.
- Tate, Tim (1990), *Child pornography*, Methuen.
- Taylor, Max (1999), *'The Nature and Dimensions of Child Pornography on the Internet'*, paper delivered to conference on combating child pornography on the Internet, Vienna, 29 September – 1 October 1999.
- Von Feilitzen, Cecilia & Ulla Carlsson (eds) (2000), *Children in the New Media Landscape. Games, Pornography, Perceptions*, Göteborg: UNESCO.

B) NATIONAL PLANS OF ACTION

- Austria – Violence in society, violence in the family, maltreatment of children, sexual abuse of children, violence among teenagers and violence in the media (1997)
- Finland – Action to combat the Commercial Sexual Exploitation of children (1999)
- Germany – Working programme of the Federal Government against child abuse, child pornography and sex tourism for the national implementation of the Declaration and the Plan of Action of the World Congress against Commercial Sexual Exploitation of Children (1998)
- Italy – Piano d'azione del governo per l'infanzia e l'adolescenza (1997/1998)
- Netherlands – Nationaal Actieplan 'Bestrijding Seksueel geweld tegen kinderen' (2000)
- Sweden – National Plan of Action (1996)
- UK – National Plan for safeguarding Children from Commercial Sexual Exploitation (2001)

C) INITIAL OR PERIODIC STATE PARTY REPORTS TO THE COMMITTEE ON THE RIGHTS OF THE CHILD

- Initial report of State party: Austria 26/06/97 – CRC/C/11/Add.14
Initial report of State party: Belgium 06/09/94 – CRC/C/11/Add.3
Initial report of State party: Denmark 12/10/93 – CRC/C/8/Add.8
Initial report of State party: Finland 30/01/95 – CRC/C/8/Add.22
Initial report of State party: France 04/06/93 – CRC/C/3/Add.15
Initial report of State party: Germany 16/09/94 – CRC/C/11/Add.5
Initial report of State party: Greece 25/06/01 – CRC/C/28/Add.17
Initial report of State party: Ireland 17/06/96 – CRC/C/11/Add.12
Initial report of State party: Italy 20/02/95 – CRC/C/8/Add.18
Initial report of State party: Luxembourg 11/04/97 – CRC/C/41/Add.2
Initial report of State party: Netherlands 24/07/97 – CRC/C/51/Add.1
Initial report of State party: Portugal 16/09/94 – CRC/C/3/Add.30
Initial report of State party: Spain 26/10/93 – CRC/C/8/Add.6
Initial report of State party: Sweden 23/09/92 – CRC/C/3/Add.1
Initial report of State party: UK 28/03/94 – CRC/C/11/Add.1
Periodic report of State Party: Belgium 25/10/00 – CRC/C/83/Add.2
Periodic report of State Party: Denmark 31/03/00 – CRC/C/70/Add.6
Periodic report of State Party: Finland 18/11/98 – CRC/C/70/Add.3
Periodic report of State Party: Portugal 26/02/01 – CRC/C/65/Add.11
Periodic report of State Party: Spain 12/11/01 – CRC/C/70/Add.9
Periodic report of State Party: Sweden 11/02/98 – CRC/C/ 65/Add.3
Periodic report of State Party: UK 25/02/02 – CRC/C/83/Add.3

D) REPORTS

Progress report n°1 – Safer Internet Action Plan Reporting – Project EDUCAUNET (2000)

Progress report n°1 – Safer Internet Action Plan Reporting – Project Friendly Internet ADICONSUM – Italian Association for Consumers and Environment Protection (2001)

Partners: TIN.IT, VKI-Konsument, SCC-Swedish Consumer Coalition, AGE – Associazione Italiana Genitori, UCIIM – Unione Italiana Insegnanti Cattolici Medi, Caetani Institute

Progress report n°1 – Safer Internet Action Plan Reporting – Project S.I.F.Kal.

Universidad de Cadiz

Partners: Extreme Media Solutions (Greece); Universidad internacional de Andalucia (Spain); Universidad de las islas Baleares (Spain); University of East Anglia (UK); Universität des Saarlandes (Denmark); Gesellschaft für Medienpädagogik und Kommunikationskultur (Denmark)

Progress report n°2 – Safer Internet Action Plan Reporting Form – Project Safer Use of Services on the Internet (SUSI)

Learning and Teaching Scotland

Partners: Scottish Parent Teacher Council (UK); Euskaltel and Euskaltel Fundacion (Spain); Heimili og Skoli (Iceland); Vereniging voor Openbaar Onderwijs (Netherlands) (2001)

Progress report n°1 – Safer Internet Action Plan Reporting Form – Project ONCE (2002)

University of Central Lancashire (UK)

Partners: University of Namur (Belgium); Dublin City University (Ireland); Hellenic Consumer Organization (Greece)

Final Report – Project SUI

Awareness program in Austria, Finland and Spain (2001)

Final Report – Project Info Net

Information on safer Internet to Italian and Spanish users (2001)

Rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant l'application de la recommandation du Conseil du 24 septembre 1998 sur la protection des mineurs et de la dignité humaine – COM (2001) 106 final

Intermediate Evaluation of the Safer Internet Action Plan BDCR (Business Development Research Consultants) Conducted by the European Commission, Volume 1 & volume 2, Final report (2001)

Self-regulation of Internet Content – Bertelsmann Foundation (1999)

E) BULLETINS

Eurochild News – 1999, 2000, 2001

News on Children, and violence on the screen – volume 3, N°1, 1999 The Unesco International clearinghouse on Children and violence on the Screen

Safer Internet – Newsletter for awareness Raisers in the EU Safer Internet programme, (from March 2001 to June 2003)

AREA OF INTERVENTION D (TECHNOLOGICAL MEASURES)

CERT Coordination Center Anonymous FTP Abuses

http://www.cert.org/tech_tips/anonymous_ftp_abuses.html

Chat Wise, Street Wise – Children and Internet Chat Services,

A paper prepared by the Internet Crime Forum IRC sub-group

http://www.internetcrimeforum.org.uk/chatwise_streetwise.html

CSIRO, Commonwealth Scientific & Industrial Research Organization
Access Prevention Techniques for Internet Content Filtering
Prepared for the National Office for the Information Economy
<http://www.cmis.csiro.au/Reports/filtering.pdf>

ECPAT

www.ecpat.net

Child Pornography written by John Carr for ECPAT
http://www.focalpointngo.org/yokohama/PDF/en/Yokohama/Background_reading/Theme_papers/Theme%20paper%20Child%20Pornography.pdf

EFA

Content Rating and Filtering
<http://www.efa.org.au/Issues/Censor/cens2.html>

En Lutte Contre la Pédophilie sur Internet : le projet MAPI

La Pornographie Infantile sur Internet
<http://www.info.fundp.ac.be/~mapi/mapi-fr.html>

High Technology Crime Investigation Association (HTCIA) International

HTCIA International, The monthly publication for the members of the High
Technology Crime Investigation Association
<http://www.htcia.org/>

House of the Dead .org

Fighting Child Pornography online
<http://www.houseofthedeath.org/>

LINX Content Regulation Committee

LINX Best Current Practice – Traceability
Version 1.0, last modified 18th May, 1999
<http://www.linx.net/noncore/bcp/traceability-bcp.html>

newIRCusers.com

Chatting on the Net

The Information Source for Internet Relay Chat, Webpage Chart and Instant
Messaging Chat

<http://www.newircusers.com/ircchat.html>

PERKEO

Data Scanner, Against Child Pornography and Animal Pornography

<http://www.perkeo.de/>

Random Art

IP Tracking Tutorial

<http://www.random-art.com/tutorial/iptracking.htm>

Safer Internet.org

<http://www.saferinternet.org/index.asp>

Scientific American

Filtering Information on the Internet

By Paul Resnick

<http://www.sciam.com>

Stanford Computer Science Education -- CSE

Filtering and Pornography

<http://cse.stanford.edu/classes/cs201/projects-98-99/online-pornography/index.html>

Test Aankoop Nr. 452 - Maart 2002 Test van 18 internetfilters Wat glipt er door de mazen van het net?

The Computer Laboratory, the Computer Science department of the University of Cambridge (Richard Clayton University of Cambridge, Computer Laboratory, Gates Building, JJ Thompson Avenue, Cambridge CB3 0FD, United Kingdom)

The Limits of Traceability

http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html

The New York Times

02/04/2001

Compressed Data Law Newsletter has to Sneak Past Filters

USA Today

14/02/2002

Town gets caught in a porn-less Net

Usus The usually useful Internet Guide for Journalists

Elements of the Net

<http://www.usus.org/elements>

WeirNet Tracing Email / How Spammers Find you

<http://www.weir.net/WeirNet/support/faq/antispam/tracing.html>

13.

(ANNEXES REGARDING AREA OF INTERVENTION A DETECTION AND CONTROL)**ANNEX 1****QUESTIONNAIRE ON DETECTION/CONTROL MEASURES AGAINST CHILD PORNOGRAPHY ON THE INTERNET**

The questionnaire is divided into four parts:

- *Criminal law measures*: the aim is to understand whether specific child pornography offences have been enacted and, if so, which conducts are criminalised and which sanctions are provided;
- *Investigative and judicial measures*: the aim is to acquire information on the existence and structure of specialised law enforcement units and on the use of special means of investigation;
- *International co-operation* in the investigation and prosecution of child pornography offences;
- *Responsibility of Internet Service Providers* in relation to child pornography material distributed through them.

A. CRIMINAL LAW MEASURES**SPECIFIC OFFENCE**

1. Does a separate criminal offence on 'child pornography' exist in your country?

<input type="checkbox"/>	Yes (please go to question n. 2)
<input type="checkbox"/>	No (please go directly to question n. 12)

2. Does the definition of 'child pornography' include pornographic material that visually depicts (please tick one or more answers as appropriate):

- a minor/child engaged in sexually explicit conduct;
- a person appearing to be a minor engaged in sexually explicit conduct;
- realistic images representing a minor engaged in sexually explicit conduct
- depictions of child pornography in drawing/cartoon form
- child pornographic text

3. Which of the following conducts, related to child pornography, are considered an offence in your country? (please tick one or more answers as appropriate)

- producing child pornography for the purpose of its distribution through a computer system;
- offering or making available child pornography through a computer system;
- distributing or transmitting child pornography through a computer system;
- procuring child pornography through a computer system for oneself or for another;

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

3.1 What are the respective penalties (minimum/maximum) for each of these conducts?

4. Does the crime of child pornography also include 'virtual' child pornography (i.e., pornographic material created either by manipulating existing pictures or by producing a combined image from different pictures, or even entirely computer-generated)?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

5. The term "minor" or "child" in relation to child pornography shall include:

- All persons under 18 years of age;
 All persons under 16 years of age;
 Other (please specify)

6. Are the following conducts considered as aggravating circumstances? (please tick one or more answers as appropriate)

- it involves depictions of a child below the age of (please put years), or
 it involves depictions of a child being exposed to violence or force, or
 it generates substantial proceeds, or
 it is committed within the framework of a criminal organisation
 other (please specify)

6.1 If any of these is considered as an aggravating circumstance, how much is the penalty increased?

7. Does your country's legislation prohibit natural persons from exercising, temporarily or permanently, activities related to the supervision of children, where they have been convicted of an offence referred to child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

8. For crimes concerning the child pornography, do provisions exist requiring confiscation, where appropriate, of the instruments and proceeds of those offences?

Instruments of the crime	Yes <input type="checkbox"/> No <input type="checkbox"/>
Proceeds of the crime	Yes <input type="checkbox"/> No <input type="checkbox"/>

9. Can a legal person (e.g. corporations) be held liable for child pornography offences?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

9.1 If yes, under which conditions?

10. What sanctions are provided for legal persons held liable for offences related to child pornography?

- Criminal sanctions (please specify)

Non-criminal sanctions (please specify)

11. Does your country legislation provide for the temporary or permanent closure of establishments which have been used or intended for committing these offences?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

(Please now go directly to question n. 19)

12. (From question n. 1) Does a definition exist of 'sexual exploitation' in relation to a child, which includes the exploitative use of children in pornographic performances and materials, including the production, sale and distribution or other forms of trafficking in such materials, and the possession of such materials?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

12.1 If such definition exists, is this form of sexual exploitation of children classified as a criminal offence?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

13. Does your country provide for custodial penalties for the sexual exploitation of children?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

13.1 If custodial penalties are provided, what are they?

14. Do measures exist that, for crimes concerning the sexual exploitation of children (with the exception of the conduct of possession of child pornography materials), sanction participation and attempt?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

15. For crimes concerning the sexual exploitation of children, do provisions exist requiring confiscation, where appropriate, of the instruments and proceeds of those offences?

Instruments of the crime	Yes <input type="checkbox"/> No <input type="checkbox"/>
Proceeds of the crime	Yes <input type="checkbox"/> No <input type="checkbox"/>

16. Can a legal person be held liable for children sexual exploitation offences?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

16.1 If yes, under which conditions?

17. What sanctions are provided for legal persons held liable for offences related to children sexual exploitation? (please tick one or more answers as appropriate)

Criminal sanctions (please specify)

Non-criminal sanctions (please specify)

18. Does your country legislation provide for the temporary or permanent closure of establishments which have been used or intended for committing these offences?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

B. INVESTIGATIVE AND JUDICIAL MEASURES

(In this section please regard the terms "Child pornography" and "Sexual exploitation of children" as exchangeable)

19. Does a specialised unit exist within law enforcement authorities in your country to deal with information on suspected production, processing, distribution and possession of child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

19.1 If such unit exists, how is it organised (e.g., number of staff, their background)?

20. What kind of specific training is provided for the officials of the specialised unit?

21. Do measures exist encouraging Internet users to inform law enforcement authorities on suspected distribution of child pornography material on the Internet?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

22. Does a law enforcement web site exist where users can report on potentially illegal material on the Internet?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

Please, provide the Internet address

23. Does any form of co-operation exist between the specialised law enforcement unit and private foundations or associations which combat child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

23.1 If yes, please describe it briefly

24. Is there any co-ordination among the authorities responsible for the fight against the sexual exploitation of children (Ministerial Departments, police forces, judicial authorities specialised in the matter, public bodies with responsibility in the matter)?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

24.1 If yes, please describe it briefly

25. Do the national services (e.g. immigration, social security, tax authorities), which are likely to have relevant experience in the context of sexual exploitation of the children, cooperate with the authorities responsible of the investigation and punishment of child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

25.1 If so, how?

SPECIAL TECHNIQUES OF INVESTIGATION

26. What kind of operational police methods and techniques are used and/or foreseen in your legislation? (please tick one or more answers as appropriate)

- Wiretapping
- Undercover operations
- Surveillance
- Controlled deliveries
- Sting operations or provocations
- Other (please specify)

27. Do legislative or other measures exist which empower the competent authorities to search or similarly access

a computer system or part of it?	Yes <input type="checkbox"/> No <input type="checkbox"/>
a computer–data storage medium in which computer data may be stored?	Yes <input type="checkbox"/> No <input type="checkbox"/>

28. Do legislative or other measures exist empowering the competent authorities to seize or similarly secure computer data accessed?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

29. Do measures exist allowing law enforcement authorities to defer action if and as long as tactically necessary, for instance with a view to getting at those behind the criminal operations, or at networks (child pornography rings) ?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

30. Do measures exist enabling the competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

31. Do measures exist enabling the competent authorities to oblige the person in possession of stored computer data to maintain the integrity of that computer data for a period of time as long as necessary?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

32. Do measures exist ensuring the expeditious preservation of traffic data and its expeditious disclosure to the competent authorities?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

33. Do measures exist empowering the competent authorities to order a person to submit specified computer data in that person's possession or control?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

34. Do measures exist empowering the competent authorities to order a service provider offering its services on its territory to submit subscriber information relating to such services?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

35. Do measures exist empowering the competent authorities to collect and record traffic data, in real-time, through the application of technical means on their territory?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

36. Do measures exist empowering the competent authorities to collect and record content data, in real-time, through the application of technical means on their territory?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

37. Do measures exist empowering the competent authorities to compel a service provider, within its technical possibilities?

to collect or record traffic data in real-time?	Yes <input type="checkbox"/> No <input type="checkbox"/>
to cooperate and assist the competent authorities in the collection or recording of traffic data in real-time?	Yes <input type="checkbox"/> No <input type="checkbox"/>

38. Do measures exist empowering the competent authorities to compel a service provider, within its technical possibilities

to collect or record content data in real-time?	Yes <input type="checkbox"/> No <input type="checkbox"/>
to cooperate and assist the competent authorities in the collection or recording of content data in real-time?	Yes <input type="checkbox"/> No <input type="checkbox"/>

C. INTERNATIONAL CO-OPERATION

39. Do measures exist allowing direct transmission of requests for assistance between locally competent authorities?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

40. Do measures exist allowing, in urgent circumstances, to make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

41. Do measures exist allowing the spontaneous supply to other Member States of information useful to begin or carry out an investigation?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

42. Does an operational point of contact exist among other EU Member States for the purpose of exchanging information in child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

42.1 If such point of contact exists, please write name and address

42.2 Is it functioning on a 24-hour basis?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

43. Do you inform Europol of suspected cases of child pornography?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

44. Is double criminality a prerequisite for co-operation with other Member States?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

45. Is child pornography an extraditable offence?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

46. Do measures exist establishing jurisdiction over child pornography offences?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

46.1 If such measures exist, in which of the following cases are your authorities competent?

- the offence is committed in whole or in part within its territory; or
- the offender is one of its nationals; or
- the offence is committed for the benefit of a legal person established in the territory of that Member State

47. Is a specific and quick procedure provided for the letters rogatory which come from other EU Member States regarding child pornography on the Internet?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

47.1 If so, what is it and how does it function?

D. RESPONSIBILITY OF INTERNET SERVICE PROVIDERS

48. Do measures exist which impose a duty on Internet providers to advise the competent authorities of the specialised law enforcement unit of child pornography material of which they have been informed or of which they are aware and which is distributed through them?

- Yes, sanctioned with criminal sanctions (please specify);
- Yes, sanctioned with administrative sanctions (please specify);
- No
- No, but a draft law exists to introduce such duty

49. Do measures exist which impose a duty on Internet providers to withdraw from circulation child pornography material of which they have been informed or of which they are aware and which is distributed through them, unless otherwise specified by the competent authorities?

- Yes, sanctioned with criminal sanctions (please specify);
- Yes, sanctioned with administrative sanctions (please specify);
- No
- No, but a draft law exists to introduce such duty

50. Do measures exist which impose a duty on Internet providers to retain traffic-data, where applicable and technically feasible for such time as may be specified under the applicable national law, to allow the data to be made available for inspection by the criminal prosecution authorities?

- Yes, sanctioned with criminal sanctions (please specify);
- Yes, sanctioned with administrative sanctions (please specify);
- No
- No, but a draft law exists to introduce such duty

51. Do measures exist which impose a duty on Internet providers to set up their own control systems for combating the production, processing, possession and distribution of child pornography material?

- Yes, sanctioned with criminal sanctions (please specify);
- Yes, sanctioned with administrative sanctions (please specify);
- No
- No, but a draft law exists to introduce such duty

ANNEX 2
SYNOPTIC TABLES FOR THE MAPPING ACTIVITY

The number in the tables corresponds to the question asked in Questionnaire A.1.

CRIMINAL LAW MEASURES

	<i>1. Separate criminal offence related to 'child pornography'</i>	<i>2. Definition of 'child pornography' or 'sexual exploitation of children' includes:</i>	<i>3. Conducts established as criminal offences</i>	<i>3.1. Sanctions</i>	<i>5. Definition of 'minor'</i>
AUSTRIA	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Depictions of child pornography in drawing/cartoon form	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	No minimum penalties Maximum 2 years of imprisonment For possession, up to 6 months of imprisonment	All persons under 14 years of age
BELGIUM	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Depictions of child pornography in drawing/cartoon form	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	From a) to d) imprisonment 5–10 years + fine Euro 25–250 (x200) For e) imprisonment 1 month–1 year + fine Euro 25–250	All persons under 18 years of age

	<i>1. Separate criminal offence related to 'child pornography'</i>	<i>2. Definition of 'child pornography' or 'sexual exploitation of children' includes:</i>	<i>3. Conducts established as criminal offences</i>	<i>3.1. Sanctions</i>	<i>5. Definition of 'minor'</i>
DENMARK	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct;	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Possessing child pornography The crime also includes 'virtual' child pornography	For a), b) and c) imprisonment up to 2 years + fine For d) imprisonment up to 6 months + fine	All persons under 18 years of age
FINLAND	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	For c) imprisonment up to 2 years + fine For e) imprisonment up to 6 months + fine	All persons under 18 years of age
FRANCE	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Depictions of child pornography in drawing/cartoon form e) Child pornographic text	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	For a) imprisonment up to 3 years + fine up to Euro 45.000 For b) and c) imprisonment up to 5 years + fine up to Euro 75.000 For d) and e) imprisonment up to 2 years + fine up to Euro 30.000	All persons under 18 years of age

	<i>1. Separate criminal offence related to 'child pornography'</i>	<i>2. Definition of 'child pornography' or 'sexual exploitation of children' includes:</i>	<i>3. Conducts established as criminal offences</i>	<i>3.1. Sanctions</i>	<i>5. Definition of 'minor'</i>
GERMANY	Yes	a) A minor engaged in sexually explicit conduct; Also b) Depictions of child pornography in drawing/cartoon form c) Child pornographic text	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	3 months to 5 years imprisonment	All persons under 14 years of age
GREECE	No	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Depictions of child pornography in drawing/cartoon form e) Child pornographic text	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography The crime also includes 'virtual' child pornography	-	All persons under 17 years of age
IRELAND	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Child pornographic text	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	For e), imprisonment up to 5 years, for a) and c) imprisonment up to 14 years	All persons under 17 years of age

	<i>1. Separate criminal offence related to 'child pornography'</i>	<i>2. Definition of 'child pornography' or 'sexual exploitation of children' includes:</i>	<i>3. Conducts established as criminal offences</i>	<i>3.1. Sanctions</i>	<i>5. Definition of 'minor'</i>
ITALY	Yes	a) A minor engaged in sexually explicit conduct; b) Realistic images representing a minor engaged in sexually explicit conduct	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime does not include 'virtual' child pornography	For a) imprisonment from 6 to 12 years. For b), c) and d) imprisonment from 1 to 5 years For e) imprisonment from 1 to 3 years	All persons under 18 years of age
LUXEMBOURG	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct; c) Realistic images representing a minor engaged in sexually explicit conduct Also d) Depictions of child pornography in drawing/cartoon form e) Child pornographic text	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	Imprisonment from 3 months to 5 years + fine from Euro 500 to 500.000	All persons under 18 years of age
THE NETHERLANDS	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct;	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Possessing child pornography The crime does not include 'virtual' child pornography	Up to 4 years imprisonment, 6 years for commercial activity	All persons under 16 years of age A draft law is going to increase this limit to 18 years of age

	<i>1. Separate criminal offence related to 'child pornography'</i>	<i>2. Definition of 'child pornography' or 'sexual exploitation of children' includes:</i>	<i>3. Conducts established as criminal offences</i>	<i>3.1. Sanctions</i>	<i>5. Definition of 'minor'</i>
PORTUGAL	No	-	-	-	All persons under 18 years of age
SPAIN	Yes	a) A minor engaged in sexually explicit conduct	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography The crime does not include 'virtual' child pornography	For a) imprisonment up to 12 years. For b) and c) imprisonment from 1 up to 3 years.	All persons under 18 years of age
SWEDEN	Yes	- A minor engaged in sexually explicit conduct; - Realistic images representing a minor engaged in sexually explicit conduct; - Depictions of child pornography in drawing/cartoon form; - Child pornographic text.	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Procuring child pornography e) Possessing child pornography The crime also includes 'virtual' child pornography	Minor crime: fine – 6 month imprisonment; For b) imprisonment for a maximum of 2 years. Serious crime: imprisonment from 6 months to 4 years.	18 years
UNITED KINGDOM	Yes	a) A minor engaged in sexually explicit conduct; b) A person appearing to be minor engaged in sexually explicit conduct;	a) Producing child pornography b) Offering or making available child pornography c) Distributing child pornography d) Possessing child pornography The crime includes 'virtual' child pornography	For a), b) and c) imprisonment up to 10 years For d) imprisonment up to 5 years	All persons under 15 years of age

	6. Aggravating circumstances	7. Measures prohibiting natural persons from exercising activities related to the supervision of children	8. Confiscation of the instruments and proceeds from the crime	9–10. Corporate liability (either administrative or criminal)	11. Temporary or permanent closure of establishments been used or intended for committing the offence
AUSTRIA	The crime is committed within framework of a criminal organisation. Penalty increased to a maximum up to 3 years imprisonment	No	a) Instruments b) proceeds	No	-
BELGIUM	The crime is committed within framework of a criminal organisation. Imprisonment 10–15 years + fine Euro 125–1250 (for all categories except possession)	Yes	a) Instruments b) proceeds	Yes Non-criminal sanctions: only civil liability when the offence happens with material provided by the corporation/firm	Yes
DENMARK	The crime generates substantial proceeds, or is committed within framework of a criminal organisation.	Yes	a) Instruments b) Proceeds	No	-
FINLAND	The production of child pornography also includes aggravated sexual abuse of the child. Imprisonment from 1 up to 10 years	No	a) Instruments b) proceeds	No	No
FRANCE	-	Yes	a) Instruments b) proceeds	Yes Criminal and non-criminal sanctions	Yes
GERMANY	The crime generates substantial proceeds, it is committed within framework of a criminal organisation or it depicts the actual sexual abuse of a child.	No	a) Instruments b) proceeds	No	-

	6. Aggravating circumstances	7. Measures prohibiting natural persons from exercising activities related to the supervision of children	8. Confiscation of the instruments and proceeds from the crime	9–10. Corporate liability (either administrative or criminal)	11. Temporary or permanent closure of establishments been used or intended for committing the offence
GREECE	The crime involves a child below the age of 17 years, it involves depictions of a child exposed to violence or force, it generates substantial proceeds, it is committed within the framework of a criminal organisation.	Yes	a) Instruments b) proceeds	Yes Criminal sanctions	
IRELAND	No aggravating circumstances	Yes Sex Offenders Act 2001	a) Instruments b) proceeds	Yes Conditions: computers or images are in the custody of the corporation Criminal sanctions	No
ITALY	The crime involves a child below the age of 14 years, if it generates substantial proceeds, it is committed within the framework of a criminal organisation, it involves persons with parental or tutoring links with the victim	Yes	a) Instruments b) proceeds	Yes Non-criminal sanctions: revocation of public authorisations	Yes
LUXEMBOURG	The crime is committed within the framework of a criminal organisation	No	a) Instruments b) proceeds	Yes	Yes
THE NETHERLANDS	The crime involves depictions of a child below the age of 16 years (limit to be increased to 18 years)	No	a) Instruments	No	No
PORTUGAL	-	-	a) Instruments b) proceeds	Yes Criminal sanctions	Yes
SPAIN	The crime is committed within the framework of a criminal organisation The penalty is increased by 3 years	No	c) Instruments d) proceeds	No	No

	6. Aggravating circumstances	7. Measures prohibiting natural persons from exercising activities related to the supervision of children	8. Confiscation of the instruments and proceeds from the crime	9–10. Corporate liability (either administrative or criminal)	11. Temporary or permanent closure of establishments been used or intended for committing the offence
SWEDEN	The crime involves a great number of depictions of an infant, it involves depictions of a child being exposed to violence or force, it generates substantial proceeds, it is committed within the framework of a criminal organisation, a great number of images or video sequences is found.	Yes	a) Instruments b) proceeds	Yes Criminal sanctions	No
UNITED KINGDOM	-	Yes	a) Instruments b) proceeds	Yes Criminal sanctions	No

Investigative and Judicial Measures

	<i>19. Existence of specialised law enforcement unit</i>	<i>21–22. Measures encouraging Internet users to inform about potentially illegal material</i>	<i>23. Co-operation with private foundations or associations</i>	<i>24. Co-ordination among authorities responsible for the fight against child pornography</i>	<i>25. Co-operation of national services with law enforcement authorities</i>
AUSTRIA	Yes Part of a sub-department of the Ministry of the Interior. 4 CID officers, 1 officer with a law degree as head	No A law enforcement web site exists for users to report potentially illegal material	Yes Cooperation with hotline of ISPA Austria	No	No
BELGIUM	Yes Sub-unit with 3 persons who coordinate investigations and provide information	Yes A law enforcement web site exists for users to report potentially illegal material (www.fedpol.be)	Yes Sharing information with Child Focus, ECPAT	Yes Meetings to evaluate laws and rules, operational briefings, sharing of information	No
DENMARK	Yes 4 police officers under the national Commissioner of the Danish police with a special training in the fight against child pornography	Yes A law enforcement web site exists for users to report potentially illegal material (www.politi.dk)	Yes	No	No
FINLAND	Yes 1 officer currently working full time. Pre-trial investigations are conducted by the local police departments. A specialised IT unit is responsible for home searches in computers and similar activities	Yes A law enforcement web site exists for users to report potentially illegal material (e-mail: vihje.krp.poliisi.fi)	Yes	No	No
FRANCE	Yes	No A law enforcement web site exists for users to report potentially illegal material (www.internet-mineurs.gouv.fr)	No	No	Yes

	<i>19. Existence of specialised law enforcement unit</i>	<i>21–22. Measures encouraging Internet users to inform about potentially illegal material</i>	<i>23. Co-operation with private foundations or associations</i>	<i>24. Co-ordination among authorities responsible for the fight against child pornography</i>	<i>25. Co-operation of national services with law enforcement authorities</i>
GERMANY	Yes Federal level: 14 staff State level: 16 units in the Länder	No A law enforcement web site exists for users to report potentially illegal material (e-mail: info@bka.de + websites of state police forces)	Yes NGOs report to the police	Yes Coordination between Federal and State police forces, also with a view of standardising methods	Yes Youth welfare departments report cases of suspected child abuse; Customs services cooperate in cases where child pornography is seized
GREECE	No	Yes No law enforcement web site exists for users to report potentially illegal material	Yes	Yes	-
IRELAND	Yes 12 persons, all police investigators. Training with Europol, on-the-job experience	Yes No law enforcement web site exists for users to report potentially illegal material	Yes Dept. Of justice, Equality and Law Reform, Internet Advisory Board	Yes Dept. Of Health and Children Hospitals – sexual assault treatment units NGOs – Rape Crisis Centre, Womens' Aid	Yes Garda National Immigration Unit
ITALY	Yes About 30 detectives Trained in criminal/forensic analysis; special studies on the matter	Yes A law enforcement web site exists for users to report potentially illegal material (www.carabinieri.it)	Yes ECPAT Italy, Unicef, Italian Parents & Family Association, Terres des Hommes, Telefono Arcobaleno, Telefono Azzurro	Yes Panel of magistrates, Interministerial Committee, Special Committee on child and adolescence problems	Yes
LUXEMBOURG	Yes Section 'Protection de la Jeunesse' from the 'Service de Police Judiciaire' Composed of 5 officers, 2 of whom specifically work on child pornography	No No law enforcement web site exists for users to report potentially illegal material	No	No	No

	<i>19. Existence of specialised law enforcement unit</i>	<i>21–22. Measures encouraging Internet users to inform about potentially illegal material</i>	<i>23. Co-operation with private foundations or associations</i>	<i>24. Co-ordination among authorities responsible for the fight against child pornography</i>	<i>25. Co-operation of national services with law enforcement authorities</i>
THE NETHERLANDS	Yes Specialised officers in 25 police regions + 5 officers at the national level	Yes No law enforcement web site yet exists for users to report potentially illegal material	Yes Public hotline Meldpunt	Yes National Plan for Action, ECPAT, NGOs	No
PORTUGAL	Yes 15 criminal investigators	Yes A law enforcement web site exists for users to report potentially illegal material (www.pj.pt)	Yes Informal depending on the case	Yes Institutional relations coordinated by the Minors Court	Yes
SPAIN	Yes	Yes A law enforcement web site exists for users to report potentially illegal material (www.policia.es and www.guardiacivil.org)	Yes Usually exchange of information via e-mail	Yes	No
SWEDEN	Yes 4 experienced detective inspectors, former child-abuse investigators, with computer skills. Training is provided in analysing digital media such as hard drives.	Yes A law enforcement web site exists for users to report potentially illegal material (e-mail childabuse@rkp.police.se)	Yes NGOs such as ECPAT, and the Swedish Save the Children hotline	Yes Through different projects trying to find ways for prevention, new legislation	Yes Exchange of information in different forums
UNITED KINGDOM	Yes 3 specialised national units: National Criminal Intelligence service, National Crime squad and National High-tech Crime Unit. Also 3 centres of excellence among the police forces	Yes	Yes Internet Watch Foundation	Yes Coordination groups have been set up to include relevant agencies	Yes They cooperate by request and may also be members of coordination groups where appropriate

	<i>26. Investigation powers</i>	<i>27. Measures to search and access a computer system</i>	<i>28. Measures to seize or secure computer data</i>	<i>29. Measures allowing law enforcement to defer action</i>	<i>30. Measures enabling to order preservation of computer data</i>	<i>31. Measures obliging to maintain the integrity of computer data</i>
AUSTRIA	a) Wiretapping (not for possession) b) Surveillance c) Search of home	-	-	-	-	-
BELGIUM	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries	Yes	Yes	Yes	Yes	Yes
DENMARK	a) Wiretapping b) Surveillance c) Controlled deliveries	Yes	Yes	Yes	Yes	No
FINLAND	a) Wiretapping b) Surveillance Wiretapping is not possible in relation to possession and distribution of child pornography. A law in preparation provides for increased investigative powers	No	Yes	Yes	Yes Not available for distribution, marketing and possession of child pornography	No
FRANCE	a) Wiretapping b) Surveillance c) Controlled deliveries	Yes	Yes	Yes	Yes	Yes

	<i>26. Investigation powers</i>	<i>27. Measures to search and access a computer system</i>	<i>28. Measures to seize or secure computer data</i>	<i>29. Measures allowing law enforcement to defer action</i>	<i>30. Measures enabling to order preservation of computer data</i>	<i>31. Measures obliging to maintain the integrity of computer data</i>
GERMANY	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries Wiretapping is not possible in relation to production, distribution and possession of child pornography.	Yes	Yes	Yes	No	No
GREECE	a) Sting operations or provocations	Yes	Yes	Yes	Yes	No
IRELAND	a) Wiretapping b) Undercover operations c) Surveillance	Yes	Yes	No	No	No
ITALY	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries	Yes	Yes	Yes	Yes	No
LUXEMBOURG	a) Wiretapping b) Surveillance c) Controlled deliveries	No	No	No	No	No

	<i>26. Investigation powers</i>	<i>27. Measures to search and access a computer system</i>	<i>28. Measures to seize or secure computer data</i>	<i>29. Measures allowing law enforcement to defer action</i>	<i>30. Measures enabling to order preservation of computer data</i>	<i>31. Measures obliging to maintain the integrity of computer data</i>
THE NETHERLANDS	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries	Yes	Yes	Yes	-	-
PORTUGAL	a) Undercover operations b) Surveillance c) Controlled deliveries	Yes	Yes	Yes	Yes	Yes
SPAIN	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries	Yes	Yes	Yes	Yes	Yes
SWEDEN	a) Undercover operations b) Surveillance c) Controlled deliveries	Yes	Yes	Yes	No	No
UNITED KINGDOM	a) Wiretapping b) Undercover operations c) Surveillance d) Controlled deliveries e) Sting operations or provocations	Yes	Yes	Yes	Yes	Yes

	<i>32. Measures ensuring the expeditious preservation of traffic data</i>	<i>33. Measures ordering a person to submit specified computer data in one's control</i>	<i>34. Measures ordering a service provider to submit subscriber information</i>	<i>35. Measures empowering law enforcement to collect/record traffic data</i>	<i>36. Measures empowering law enforcement to collect/record content data in real-time</i>	<i>37. Measures empowering law enforcement to collect/record content data in real-time</i>	<i>38. Measures empowering law enforcement to collect/record content data in real-time</i>
AUSTRIA	-	-	-	-	-	-	-
BELGIUM	Yes	Yes	Yes	-	Yes	Yes	Yes
DENMARK	Yes	No	Yes	Yes	Yes	Yes	Yes
FINLAND	Yes for production of child pornography. Not available for distribution, marketing and possession of child pornography	No	Yes Police Act, section 36	Yes for production of child pornography. Not available for distribution, marketing and possession of child pornography	No	Yes Coercive Measures Act, Chapter 5a, Section 9. Duty to help and assist of a telecommunications service	Yes
FRANCE	No	Yes	Yes	Yes	Yes	Yes	Yes
GERMANY	No	-	Yes	Yes	Yes	Yes	Yes
GREECE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IRELAND	No	No	No	No	No	No	No
ITALY	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LUXEMBOURG	No	No	No	No	No	No	No
THE NETHERLANDS	-	-	Yes	Yes	Yes	Yes	-
PORTUGAL	No	Yes	Yes	Yes	Yes	Yes	Yes
SPAIN	No	Yes	Yes	Yes	Yes	Yes	Yes

	<i>32. Measures ensuring the expeditious preservation of traffic data</i>	<i>33. Measures ordering a person to submit specified computer data in one's control</i>	<i>34. Measures ordering a service provider to submit subscriber information</i>	<i>35. Measures empowering law enforcement to collect/record traffic data</i>	<i>36. Measures empowering law enforcement to collect/record content data in real-time</i>	<i>37. Measures empowering law enforcement to collect/record content data in real-time</i>	<i>38. Measures empowering law enforcement to collect/record content data in real-time</i>
SWEDEN	Yes	Yes	Yes	No	No	No for measures to compel a service provider to collect or record traffic-data in real-time. Yes for measures to compel a service provider to cooperate and assist in the collection or recording of traffic-data in real-time.	No for measures to compel a service provider to collect or record content data in real-time. Yes for measures to compel a service provider to cooperate and assist in the collection or recording of content data in real-time.
UNITED KINGDOM	Yes	Yes	Yes	Yes	Yes	Yes	Yes

International Cooperation

	<i>39. Request for assistance</i>	<i>40. Make urgent requests for mutual assistance</i>	<i>41. Supply information to other Member States</i>	<i>42. Inform Europol of suspected cases</i>	<i>43. Dual criminality prerequisite for cooperation</i>	<i>44. Measures establishing jurisdiction over child pornography offences</i>	<i>45. Specific and quick procedure provided for letters rogatory regarding child pornography on the Internet cases</i>
AUSTRIA	Yes	Yes	Yes	No	-	-	Yes
BELGIUM	Yes	Yes	Yes	Yes	No	Yes If the offender is one of its nationals	Yes Directly from magistrate to magistrate - In the near future through Eurojust
DENMARK	Yes	Yes	Yes	Yes	Yes	Yes If the offence is committed in whole or in part within its territory	No
FINLAND	No. Available only with Nordic countries (Denmark, Iceland, Norway, Finland and Sweden)	Yes	Yes	No	Yes	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals	No

	<i>39. Request for assistance</i>	<i>40. Make urgent requests for mutual assistance</i>	<i>41. Supply information to other Member States</i>	<i>42. Inform Europol of suspected cases</i>	<i>43. Dual criminality prerequisite for cooperation</i>	<i>44. Measures establishing jurisdiction over child pornography offences</i>	<i>45. Specific and quick procedure provided for letters rogatory regarding child pornography on the Internet cases</i>
FRANCE	Yes	Yes	Yes	No	Yes	No	No
GERMANY	Yes	Yes	Yes	No	No	-	Yes Through police channels
GREECE	Yes	Yes	Yes	Yes	No	No	No
IRELAND	Yes	Yes	Yes	Yes	No	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals	No
ITALY	Yes	No	Yes	Yes	No	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals, or if the offence is committed for the benefit of a legal person established in its territory	Yes Liaison magistrate on duty, activated through the Ministry of Justice or through its delegated officers

	<i>39. Request for assistance</i>	<i>40. Make urgent requests for mutual assistance</i>	<i>41. Supply information to other Member States</i>	<i>42. Inform Europol of suspected cases</i>	<i>43. Dual criminality prerequisite for cooperation</i>	<i>44. Measures establishing jurisdiction over child pornography offences</i>	<i>45. Specific and quick procedure provided for letters rogatory regarding child pornography on the Internet cases</i>
LUXEMBOURG	Yes	Yes	Yes	-	Yes	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals, or if the offence is committed for the benefit of a legal person established in its territory	No
THE NETHERLANDS	Yes	Yes	Yes	Yes	Yes	Yes If the offence is committed for the benefit of a legal person established in its territory	Yes Via LICC and the regional ICC offices
PORTUGAL	Yes	Yes	Yes	Yes	Yes	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals	No

	<i>39. Request for assistance</i>	<i>40. Make urgent requests for mutual assistance</i>	<i>41. Supply information to other Member States</i>	<i>42. Inform Europol of suspected cases</i>	<i>43. Dual criminality prerequisite for cooperation</i>	<i>44. Measures establishing jurisdiction over child pornography offences</i>	<i>45. Specific and quick procedure provided for letters rogatory regarding child pornography on the Internet cases</i>
SPAIN	Yes	No	Yes	No	Yes	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals, or if the offence is committed for the benefit of a legal person established in its territory	No
SWEDEN	Yes	Yes	Yes	Yes	No	Yes If the offence is committed in whole or in part within its territory or if the offender is one of its nationals.	Yes
UNITED KINGDOM	Yes	Yes	Yes	Yes	No	No	No

Liability of Internet Service Providers

	<i>46. Measures imposing duties on ISPs to advise law enforcement authorities of child pornography material distributed through them</i>	<i>47. Measures imposing duties on ISPs to withdraw from circulation child pornography material distributed through them</i>	<i>48. Measures imposing duties on ISPs to retain traffic data to allow them to be available for inspection by criminal prosecution authorities</i>	<i>49. Measures imposing duties on ISPs to set up their own control systems for combating production, processing, possession and distribution of child pornography material</i>
AUSTRIA	No	No	No	No
BELGIUM	Yes Criminal sanctions (technical details to be agreed in a royal decree)	Yes Criminal sanctions (technical details to be agreed in a royal decree)	Yes Criminal sanctions (technical details to be agreed in a royal decree)	No
DENMARK	Yes Criminal sanctions for aiding and abetting a crime	No	Yes	No
FINLAND	No	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty	No
FRANCE	No	No	No	No
GERMANY	No	Yes It applies to ISPs, not to Access or Network Providers	No	No
GREECE	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty

	<i>46. Measures imposing duties on ISPs to advise law enforcement authorities of child pornography material distributed through them</i>	<i>47. Measures imposing duties on ISPs to withdraw from circulation child pornography material distributed through them</i>	<i>48. Measures imposing duties on ISPs to retain traffic data to allow them to be available for inspection by criminal prosecution authorities</i>	<i>49. Measures imposing duties on ISPs to set up their own control systems for combating production, processing, possession and distribution of child pornography material</i>
IRELAND	No	No	No	No
ITALY	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty	No A draft law exists to introduce such duty
LUXEMBOURG	No	No	No	No
THE NETHERLANDS	No	No	No	No
PORTUGAL	No	No	No	No
SPAIN	No	Yes Sanctioned with administrative sanctions (a fine).	No	No
SWEDEN	Yes	Yes	No	Yes
UNITED KINGDOM	No	Yes If ISPs are aware of child pornography which is hosted on their servers, unless it is removed they can be prosecuted for possession and distribution	No	No

ANNEX 3

QUESTIONNAIRE ON THE EVALUATION OF DETECTION/CONTROL MEASURES AGAINST CHILD PORNOGRAPHY ON THE INTERNET

The questionnaire is divided into four sections:

1. *Criminal law measures*: the aim is to collect information in to evaluate the effectiveness of the legislative measures enacted by EU Member States to tackle child pornography on the Internet
2. *Investigative and judicial measures*: the aim is to collect information to evaluate the effectiveness of the investigative and judicial measures enacted by EU Member States to tackle the child pornography on the Internet
3. *Cooperation at European Union level*: the aim is to collect information to evaluate the effectiveness of the investigative procedures and the prosecution of child pornography offences on the Internet at European Union level. Specific attention will be paid to the cooperation between law enforcement agencies and Internet Service Providers
4. *Quantitative Data*: the aim is to collect available data about the incidence of child pornography on the Internet

1. CRIMINAL LAW MEASURES

1 According to you, how do you evaluate the legal framework against child pornography existing in your country (1= not at all effective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2 According to you, how do you evaluate the adequacy of the penalties provided by the legislation against child pornography enacted in your country (1= not at all effective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3 According to you, if any definition of child pornography (or sexual exploitation in relation to a child) exists in your country, how do you evaluate its adequacy in tackling child pornography on the Internet (1= not at all adequate, 2= scarcely adequate, 3= adequate, 4= very adequate)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. According to you, if any legislative provision exists in your country, prohibiting natural persons who have been convicted of an offence related to child pornography from exercising, temporarily or permanently, activities related to the supervision of children, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. According to you, if any legislative provision exists in your country requiring confiscation, where appropriate, of the instruments and proceeds for crimes concerning child pornography (or sexual exploitation of children), how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. According to you, if any legislative provision exists in your country sanctioning legal entity liability for child pornography offences (or sexual exploitation of children), how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. According to you, if any legislative provision exists in your country providing for the temporary or permanent closure of establishments that have been used or are intended for committing child pornography offences, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. INVESTIGATIVE AND JUDICIAL MEASURES

(In this section please regard the terms "Child pornography" and "Sexual exploitation of children" as exchangeable)

8. According to you, if a specialised unit exists within the law enforcement authorities in your country to deal with child pornography, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4=very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9. According to you, how do you evaluate the level of training of this specialised unit (1= very low training level, 2= low training level, 3= acceptable training level, 4= high level training)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10. According to you, how do you evaluate the adequacy of *a) the human resources* and *b) the material resources* devoted by your country, to the investigation of child pornography on the Internet (1= not adequate, 2= sufficient 3= adequate, 4= highly adequate).

Human resources

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Material resources

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

11. According to you, how do you evaluate the usefulness of the existence of reporting initiatives by Internet users to law enforcement authorities (1= not at all useful, 2= quite useful, 3= useful, 4 =very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

12. If any form of cooperation exists in your country between law enforcement and private foundations or associations, how do you rate that cooperation in tackling child pornography on the Internet? (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. According to you, if any coordination exists in your country among the authorities specifically responsible for the fight against the sexual exploitation of children (Ministerial Departments, police forces, judicial authorities specialised in the matter, public bodies with responsibility in the matter) how do you rate that coordination in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

14. According to you, if cooperation between national services (e.g. immigration, social security, tax authorities) and the law enforcement authorities exists in your country, how do you rate that cooperation in tackling child pornography on the Internet (1 = not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

15. According to you, how do you evaluate the usefulness of the measures enacted by your country empowering the competent authorities to investigate child pornography on the Internet (1 = not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

16. According to you, if any legislative provision, or other measures, exist in your country, which empower competent authorities to search or similarly access a computer system or a computer storage medium, how do you rate the usefulness of such provision/measures in tackling child pornography on the Internet (1 = not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

17 According to you, if any legislative provision, or other measures, exists in your country empowering competent authorities to seize or similarly secure computer data they have accessed, how do you evaluate its usefulness in tackling child pornography on the Internet (1 = not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

18. According to you, if any measure exists in your country allowing law enforcement authorities to defer action if and as for long as tactically necessary (for instance with a view to identifying those behind criminal operations, or networks of child pornography rings) how do you evaluate its usefulness in tackling child pornography on the Internet (1 = not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

19. According to you, if any measure exists in your country enabling competent authorities to order or similarly obtain the preservation of specified computer data, including traffic data that has been stored by means of a computer system, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

20. According to you, if any measure exists in your country enabling competent authorities to oblige the person in possession of stored computer data to maintain the integrity of that computer data for an indefinite period of time, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

21. According to you, if any measure exists in your country ensuring the expeditious preservation of traffic data and its disclosure to competent authorities, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

22. According to you, if any measure exists in your country empowering competent authorities to order a person to submit specified computer data in that person's possession or control, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

23. According to you, if any measure exists in your country empowering competent authorities to order a service provider offering its services on its territory to submit subscriber information relating to such services, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

24. According to you, if any measure exists in your country empowering competent authorities to collect and record traffic data, in real-time, through the application of technical means in their territory, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2 = quite useful, 3 = useful, 4 = very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

25. According to you, if any measure exists in your country empowering competent authorities to collect and record content data, in real-time, through the application of technical means on their territory, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

26. According to you, if any measure exists in your country empowering competent authorities to compel a service provider, within its technical possibilities, to collect or record traffic data in real-time or to cooperate and assist competent authorities in the collection or recording of traffic data in real-time, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

27. According to you, if any measure exists in your country empowering competent authorities to compel a service provider, within its technical possibilities to collect or record content data in real-time or to cooperate and assist the competent authorities in the collection or recording of content data in real-time, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. COOPERATION AT EUROPEAN LEVEL

28. According to you, if any measure exists in your country allowing the direct transmission of requests for assistance between locally competent authorities, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

29. According to you, if any measure exists in your country allowing, in urgent circumstances, the making of requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

30. According to you, if a measure exists in your country which imposes a duty on Internet providers to advise the competent authorities or specialised law enforcement unit about child pornography material of which they have been informed or are aware and which is distributed through them, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

31. According to you, if a measure exists in your country which imposes a duty on Internet providers to withdraw from circulation child pornography material they have been informed of, or are aware and which is distributed through them, unless otherwise specified by competent authorities, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

32. According to you, if a measure exists in your country which imposes a duty on Internet providers to retain traffic-data, where applicable and technically feasible for a time that may be specified by the applicable national law, to allow the data to be made available for inspection by criminal prosecution authorities, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

33. According to you, if a measure exists in your country which imposes a duty on Internet providers to set up their own control systems for combating the production, processing, possession and distribution of child pornography material, how do you evaluate its usefulness in tackling child pornography on the Internet (1= not at all useful, 2= quite useful, 3= useful, 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. QUANTITATIVE DATA

For our purpose it would be useful to know:

- a) The number of people investigated/arrested/judged or convicted in years 2001 and 2002 in your country for each of the following offences (if considered as an offence):
 - producing child pornography for the purpose of its distribution through a computer system
 - offering or making available child pornography through a computer system
 - distributing or transmitting child pornography through a computer system
 - procuring child pornography through a computer system for himself/herself or others
 - possessing child pornography in a computer system or on a computer data storage medium
- b) The number of people sanctioned with a prohibition from exercising temporarily or permanently, activities related to the supervision of children in year 2001 and 2002 in your country (if available)
- c) The number of instruments and amount of proceeds seized for crimes concerning child pornography on the Internet in years 2001 and 2002 (if available)
- d) The number of legal entities liable for child pornography offences in year 2001 and 2002 in your country (if available)
- e) The number of cases which led to the temporary or permanent closure of any establishment that have been used for committing child pornography offences in year 2001 and 2002 (if available)
- f) The number of operations carried out by the special unit in your country in 2001 and 2002 and the final consequences of the operations (arrests/convictions/seizures)
- g) The number of warnings from Internet users to the competent authorities regarding suspect child pornography websites in years 2001 and 2002 in your country and the reliability rate of these warnings

- h) The number of warnings from Internet Service Provider to the competent authorities regarding suspect child pornography websites in years 2001 and 2002 and the reliability rate of these warnings

Please send us **any other data in any available form** (as an attached file or document) you think may be useful for the aims of the Project.

ANNEX 4
SYNOPTIC TABLES FOR THE EVALUATION ACTIVITY

Results from the analysis of the questionnaire on the evaluation of the preventive measures in place in EU Member States against child pornography on the Internet.

Mean Value per question and Numerousness ¹

Dimensions	Questions	Mean Value	Numerousness
Criminal Law Measures	1	2,64	14
	2	2,21	14
	3	2,64	14
	4	2,45	11
	5	2,92	14
	6	2,8	10
	7	2,77	9
Investigative and Judicial Measures	8	3,35	14
	9	3,07	14
	10a	1,64	14
	10b	2,07	14
	11	2,8	15
	12	2,85	14
	13	3,26	15
	14	2,71	14
	15	2,6	15
	16	3,57	14
	17	3,46	15
	18	3,07	13
	19	3,28	14
	20	3,25	12
	21	3	12
	22	3,38	13
	23	3,21	14
24	3,3	13	
25	3,09	11	
26	3,23	13	
27	3,08	12	
Cooperation at European Level	28	2,85	14
	29	3,46	13
	30	3,27	11
	31	3	11
	32	2,81	11
	33	2,21	8

¹ Numerousness implies the number of valid responses for question. For the definition of valid answer

**Synoptic Tables with the results from the analysis of the questionnaire on evaluation
of the preventive measures in place in EU Member States against child pornography on the Internet (Annex 2)**

Questions	1	2	3	4	5	6	7	8	9	10a	10b	11	12	13	14	15	16
Austria	2	2	3		3			3	3	1	2	4	2	4	2	2	4
Belgium	3	1	2	4	1			4	3	2	2	3	3	3	3	2	4
Denmark	3	3	3	3	3		3	4	4	3	3	3	4	4	2	3	3
Finland	2	1	1	1	3			2	3	1	4	2	3	3		2	3
France	3	2	3	4	4	3	4	4	3	1	1	3	3	3	2	1	4
German	2	2	3	2	3	1		4				2	2	4	2	3	4
Greece									4	2	2	4	4	4	4	3	4
Ireland	3	2	3	3	2	3	2	3	3	2	2	2	2	2	3	3	4
Italy	3	3	3		4	3	3	2	3	2	2	2	3	3	3	3	3
Luxemburg	2	2	3	3	2	3	3	3	2	1	2	3		3	3	3	
the Netherlands	3	3	3	2	3	3	2	3	3	2	2	2	3	3	2	3	2
Portugal	2	2	1	1	4	4	4	4	3	2	1	4	2	4	4	3	4
Spain	3	3	3		3	2		4	3	2	2	3	3	4	3	3	4
Sweden	3	2	4	1	3	4	2	4	4	1	3	3	3	3	3	2	4
United Kingdom	3	3	2	3	3	2	2	3	2	1	1	2	3	2	2	3	3
Numerousness	14	14	14	11	14	10	9	14	14	14	14	15	14	15	14	15	14
Mean Value	2,642857	2,214286	2,642857	2,454545	2,928571	2,8	2,777778	3,357143	3,071429	1,642857	2,071429	2,8	2,857143	3,266667	2,714286	2,6	3,571429

Questions	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Austria	4	3	4	4	4	4	4					1	4		4		
Belgium	4	3	4	3	3	3	4	4	3	3	3	3	3	3			
Denmark	3	3	3			3	3	3	3	4	4	4	3	4	4	3	
Finland	3	3	3	3			1					1					
France	3	3	3	4	3	3	3	3	3	4	4	4	4	4	3	4	4
German	4		4	4	4	4	4	4	4	4	4	1	4	3	4	4	1
Greece	4	4	4		4	4	4	4	4	4	4	4	4				
Ireland	4	2	2	2	2	3	3	2	3	3	3	3	4	4	4	2	3
Italy	3	3	3	3	2			3	3	3	3					3	
Luxemburg	3		2	2	2	3	2	3		2	2	3	3	1	1	1	1
the Netherlands	3	2	3	3	2	3	3	3	2	2	2	3	3	3	3	2	2
Portugal	3	4	4	4	4	4	4	4	4	4	4	4	4	4	2	4	2
Spain	4	3	4	4	3	3	4	3	2	3	2	3	3	4	3	2	
Sweden	4	4				4	4	4		4		4	4	4	3	4	2
United Kingdom	3	3	3	3	3	3	2	3	3	2	2	2	2	2	2	2	2
Numerousness	15	13	14	12	12	13	14	13	11	13	12	14	13	11	11	11	8
Mean Value	3,466667	3,076923	3,285714	3,25	3	3,384615	3,214286	3,307692	3,090909	3,230769	3,083333	2,857143	3,461538	3,272727	3	2,818182	2,125

14.

ANNEXES REGARDING AREA OF INTERVENTION B (SELF-REGULATION)

ANNEX 1

QUESTIONNAIRE FOR THE MAPPING OF HOTLINES IN THE EUROPEAN UNION MEMBER STATES

INSTRUCTIONS FOR THE COMPILATION OF THE QUESTIONNAIRE

1. The questionnaire has been drafted mostly in a “Yes–No” format, or with a list of possible answers, in order to allow a quick response. When more than one answer is possible, this is expressly stated at the end of the question. **If you are compiling the questionnaire in electronic format, just click on the correct answer to tick it.**
2. In a limited number of questions the answer needs some written explanation. **If you are compiling the questionnaire in electronic format, click on the space allowed to write in it, which will expand automatically. If you are compiling it in written form, please answer the questions in a separate sheet.**

QUESTIONNAIRE FOR THE MAPPING OF HOTLINES IN THE EU MEMBER STATES

GENERAL QUESTIONS

1. As regards organisation and funding of the hotline, is it run by a:

- law enforcement agency
- other publicly owned or publicly funded body
- private industry (an Association, another independent body with industry funding)
- partly by a public, partly by a private organisation
- child welfare organisation
- other private organisation

1.1 If your hotline is not run by public authorities, are there any formal/informal links with them? Please explain.

2. What type of illegal material or activity are covered by the hotline? (please tick one or more answers as appropriate)

- child pornography
- racist or extreme political material
- other (please specify)

3. What media are covered by your activity? (please tick one or more answers as appropriate)

- the World Wide Web
- newsgroups
- Internet Relay Chat (and ICQ)
- other (please specify)

4. What is your geographical scope of interest?

- only material hosted in your country
- all material available in your country

MINIMUM STANDARDS FOR OPERATING INTERNET HOTLINES

5. Can your hotline be found easily using a search engine?

- Yes No

6. How are the hotline's web site and activity publicised (active banners linking to your web site, links from other sites, leaflets, others)? Please explain.

7. Was the web site constructed by a web designer?

Yes No

8. Are you also involved in awareness activities against child pornography on the Internet?

only on the promotion of hotlines activities

on the promotion of the hotline and more general educational activities aimed at users (including children) on how to use Internet safely

other (please specify)

9. Do you publish a periodic report of your activities?

Yes No

- 9.1 If yes, can you provide us with the web site address or with a copy of the latest report

ORGANISATION OF THE HOTLINE

10. Are there any mechanisms for receiving reports operating on a 24-hour/7 days a week basis?

Yes No

11. How many people are part of the hotline's staff? What is their background? Please explain.

12. Do they receive a specific training before starting to work? Is this training repeated periodically? Please explain.

PROCEDURE FOR HANDLING COMPLAINTS

13. How can a reporter send you a complaint? (please tick one or more answers as appropriate)

- report sheet to be filled in
- fax
- e-mail
- telephone

14. If a report sheet to be filled in is not available, are any instruction provided to the reporter as to what information should be included in the complaint?

Yes No

14.1 If yes, please explain

15. Does your hotline respond:

- to both identifiable and anonymous complaints
- only when the complainant is identifiable

16. After receiving the complaint, do you check it according to formal criteria in order to determine whether it is potentially illegal?

Yes No

16.1 If you conduct a check on it, which criteria (good practices, legal standards, both) is it based on? Please explain.

17. What action can your hotline take on the reports which are received on potentially illegal material located in your country? (please tick one or more answers as appropriate)

- Advice is given as to how to pursue the complaint
- The original poster is invited to remove the potentially illegal content
- The Internet Service Provider is advised to remove the potentially illegal content
- The law enforcement is advised of the potentially illegal content

18. Does your hotline inform the law enforcement authorities:

- of all reports received
- of all cases of suspected illegal content
- only if the report exceeds a predetermined threshold of seriousness
- only if the original poster refuses to remove the potentially illegal content

19. If possessing child pornography is illegal in your country, do you warn the reporter about it and advise to delete all potentially illegal content?

Yes No

20. Are communications prioritised according to the level of danger?

Yes No

21. Do you trace the reported content?

Yes No

22. If the reported content is located abroad, do you forward it:

- To the hotline of that country
- To the law enforcement of that country
- We do not forward it

23. Are your hotline staff protected from any legal action concerning the material that they handle by legal provisions or arrangements with law enforcement or other public authorities?

Yes No

23.1 If your staff is protected from criminal liability, what can be done with the potentially illegal content?

24. Are there any exceptions to the standard procedure of handling reports?

Yes No

24.1 If yes, in which cases is an exception made? What procedures are applied?

PRIVACY OF DATA

25. If anonymous complaints are not permitted, how does the hotline ensure the protection of personal data? Please explain.

26. Do you store personal data about reporters?

Yes

No

29.1 If you store personal data, do you ask consent by the reporter?

Yes

No

27. Who has access to personal data concerning reporters? Please explain.

28. When a complaint is forwarded to other national/foreign authorities, do you pass on the personal details of the reporter?

Yes

No

29. Do you know of any other hotlines active in your country?

Yes

No

ANNEX 2

EVALUATION QUESTIONNAIRE FOR NATIONAL HOTLINES AND THE INHOPE NETWORK

INSTRUCTIONS FOR COMPLETION

For each question please respond by marking the box that most accurately addresses the question posed. If your hotline is not part of the INHOPE network, please indicate 'NA' (not applicable) next to the unanswerable questions. These questions are both objective and subjective in nature and utilize a Likert scale to measure your perception. Each number has the following meaning:

1 = totally ineffective OR completely disagree

2 = semi-effective OR disagree

3 = effective OR agree

4 = very effective OR completely agree

THE INHOPE NETWORK PROGRAM GOALS

1. In your professional experience, how effective is INHOPE at facilitating the exchange of expertise between national hotlines? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. In your professional experience, how effective are the policies and procedures provided by INHOPE when responding to child pornography on the Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Have the best practice papers for the **exchange of reports** between hotlines been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Have the best practice papers concerning **staff welfare** been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Have the best practice papers for **membership application** been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Have the best practice papers for the **ART principles of the operation**² of a hotline been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. Have the best practice papers for the **ART-2 principles of the operation**³ of a hotline been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. Have the best practice papers for the **common statistics format** been completed?

YES	NO	Don't Know
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9. In your professional experience, how effective are the best practice papers in combating child pornography on the Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9.1 Which paper, mentioned above, does your national hotline refer to the most? _____

9.2 How frequently does your national hotline refer to these papers per month? _____

9.3 Are these best practice papers used to train new staff within your national hotline?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

9.4 Are training sessions scheduled to review these best practice papers within your national hotline?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

9.5 If yes, how many times per year are these training session conducted for your national hotline?

² Available, Reliable, Transparent (ART).

³ Accountable, Responsible and Trustworthy (ART-2).

10. In your professional experience, how effective is the INHOPE network at facilitating the exchange of reports between hotlines regarding child pornography on the Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10.1 Does INHOPE identify an effective mechanism for the exchange of reports between hotlines?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

10.2 Does INHOPE identify a secure way to exchange reports between hotlines?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

10.3 How many reports are **sent** from your hotline to other hotlines within the INHOPE network per year?

10.4 How many reports are **received** by your hotline from other hotlines within the INHOPE network per year? -----

11. INHOPE is effective in establishing working relationships with hotlines outside of the EU. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

12. INHOPE effectively facilitates increased cooperation between different stakeholder groups (e.g. ISP'S, law enforcement, NGO's and the public) on an international level. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. INHOPE has supported the growth of new hotlines throughout the EU. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

14. INHOPE is effective in educating key stakeholder groups (e.g. ISP's, law enforcement, NGO's and the public) about the importance of collaboration at the international level. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

15. Effective relationships exist between INHOPE and key stakeholder groups (e.g. ISP's, law enforcement, NGO's and the public) on an international level. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

16. INHOPE is effective in raising awareness with key stakeholders (e.g. ISP's, law enforcement, NGO's and the public) about the **INHOPE network**. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

17. INHOPE is effective in raising awareness with key stakeholders (e.g. ISP's, law enforcement, NGO's and the public) about **national hotlines**. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

18. INHOPE has reached its goal of creating a "one-stop shop"⁴ website that is utilized and recognized by many different people. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 18.1 If so, how many visitors went to **INHOPE website** during: 2001_____2002_____2003_____
- 18.2 How many visitors have you had at your **national website** during: 2001_____2002_____2003_____
- 18.3 How many visitors used the **INHOPE website as portal** to find your national website during: 2001_____2002_____2003_____
- _____ Not applicable, we do not collect these statistics

⁴ This is the language used by INHOPE to reflect the goal of creating a website where someone who wishes to report illegal or harmful content can receive all the necessary information.

19. The administration of INHOPE is conducted in an efficient manner.⁵ (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

20. The administration of INHOPE is conducted in a transparent manner. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

21. The administration of INHOPE is conducted in an accountable manner. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

22. INHOPE provides a strong basis for international cooperation between various national hotlines. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

23. INHOPE provides a strong basis for international cooperation between ISP's and hotlines. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

24. INHOPE provides a strong basis for international cooperation between law enforcement agencies and hotlines. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

⁵ Numbers 18 - 21 reflect one of the objectives of INHOPE as found in their mission statement. INHOPE Association of Internet Hotlines Providers in Europe.(May 2002) *First Report*. Available online at www.inhope.org. p. 40

NATIONAL HOTLINES

The following questions concern the work carried out by the national hotline. The same Likert scale is used for subjective questions.

- 1 = totally ineffective OR completely disagree
- 2 = semi-effective OR disagree
- 3 = effective OR agree
- 4 = very effective OR completely agree

Standards and Procedures

1. Does your hotline follow a set of identified standards regarding receiving information from other hotlines?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

2. Does your hotline follow a set of identified standards regarding sending information to other hotlines?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

3. In your professional experience, how effective are the guidelines that are followed by your hotline in combating child-pornography on the Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Awareness Raising and External Relations

4. How effective is your national hotline in promoting collaboration between many different stakeholder groups (e.g. ISP's, law enforcement, NGO's and the public)? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Our hotline has a very strong relationship⁶ with other hotlines that are part of the INHOPE network. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Our hotline has a very strong relationship with other hotlines that are **NOT** part of the INHOPE network. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. When we report child pornography to other hotlines, they respond quickly and inform us of the status of the report. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 7.1 What is the average response time?

<1 day	2-5 days	6-10 days	>11 days
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 7.2 In the last year, how many reports were sent to other hotlines that are not part of the INHOPE network?

- 7.3 In the last year, how many reports did you receive from other hotlines that are not part of the INHOPE network? -----

8. Our hotline has a very strong relationship with national ISP's. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

⁶ In the following questions, "strong relationship" signifies a relationship based on the creation of an official acknowledgement of your collaboration OR a relationship based on trust meaning that your national hotline collaborates productively with the stakeholder in question. Further, your national hotline believes that when information is passed to the other party they respond appropriately.

9. When we report child pornography to ISP's they contact us immediately to discuss its status. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10. When we report child pornography to ISP's they respond quickly by removing the content. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 10.1 What is the average response time?

<1 day	2-5 days	6-10 days	>11 days
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 10.2 In the last year, how many reports were sent to ISP's?

11. Our hotline has a very strong relationship with national law enforcement agencies (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

12. When we report child pornography to law enforcement agencies, they contact us immediately to discuss the case. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. When we report child pornography to law enforcement agencies, they respond quickly by opening investigations. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13.1 What is the average response time?

<1 day	2-5 days	6-10 days	>11 days
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13.2 In the last year, how many reports were sent to law enforcement agencies?

14. Our hotline has a very strong relationship with national child protection agencies and other NGO's. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

14.1 In the last year, how many times has your agency collaborated with child protection agencies or other NGO's?

15. Our hotline has effective policies and procedures in place to follow-up on reports and provide information regarding the action taken by the hotline to the person reporting? (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

16. How effective is your hotline at raising awareness **in general** regarding child pornography on the Internet? (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

17. How effective is your hotline at raising the awareness of parents **and other caregivers** regarding child pornography on the Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

18. How effective is your hotline at raising awareness with **children** about the dangers associated with Internet? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

19. How effective is your hotline at **external relations** and gaining increased visibility within the general public? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective

)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

20. Does your hotline have one individual who focuses on awareness campaigns and external relations?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

20.1 If not, how many hours are dedicated to awareness raising per week by your staff? _____'

20.2 How many events has your hotline attended in the last year? _____

20.3 How many events has your hotline hosted in the last year? _____

20.4 Has the number of reports received increased after one of these events?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

Anonymity

21. Does your hotline allow people to remain anonymous when reporting potentially illegal content?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

22. In your professional opinion, the option to remain anonymous increases the number of reports received from the public. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

22.1 How many reports does your hotline receive a year from people who do not wish to be contacted?_____

22.2 How many people allow your hotline to contact them even if you provide an anonymous reporting option?_____

Exchange of Expertise and Training

23. The exchange of expertise between stakeholder group (e.g. ISP's, law enforcement, NGO's and the public) is sufficient for training purposes. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

23.1 How many times per year does your hotline participate in trainings hosted by INHOPE, your national hotline or other stakeholder group? _____

23.2 How many of those are done "in-house"?_____

23.3 How many of training are done in collaboration with hotlines from other countries?_____

24. The training seminars are effective at disseminating useful and current information to its participants. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

25. The Bursary Program⁷ created by INHOPE is an effective way to train new employees. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

25.1 How many times has your hotline had the opportunity to utilize the Bursary Program since it began?

25.2 How many times has your hotline actually utilized the Bursary Program since it began? -----

Care of Staff

26. How effective is your hotline at caring for staff psychologically? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

26.1 Does your hotline provide psychological assistance to your staff free of charge by appropriately trained psychologists?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

26.2 How many times has your staff utilized the psychological assistance that is available in the last year?

27. Our hotline suffers from a very high staff turnover rate. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

⁷ Enables staff from one hotline to visit and work with a more experienced hotline for a short period.

28. The turnover rate for staff is about normal for this type of work. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

29. Our hotline is currently trying to address staff retention issues. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

General Issues

30. How effective is your hotline at collecting statistics? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

31. In your professional experience, how effective is your hotline at utilizing the statistics gathered to make the hotline more efficient? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

32. In your professional experience, how effective is the hotline at protecting staff from possible legal issues that could arise from possessing child pornography? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

33. In your professional experience, how effective are the laws in protecting hotlines from the potential illegal actions of their employees? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

34. In your professional experience, how effective are policies associated with the storage of illegal material (e.g. is the time limit sufficient to address the report in a timely manner with all parties involve)? (1=totally ineffective, 2=semi-effective, 3=effective, 4=very effective)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Non-Child Pornography related material

35. Our hotline is effective in addressing non-child pornography related material. (1=totally disagree, 2=disagree, 3=agree, 4=strongly agree)

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

36. Does your hotline provide guidance to people who report adult pornography?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

37. Does your hotline provide guidance to people who report unsolicited adult email?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

38. Does your hotline provide guidance to people who report viruses?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

39. Does your hotline provide guidance to people who report fraud?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

40. Does your hotline provide guidance to people who ask questions regarding filtering?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

ANNEX 3
MAP OF NATIONAL INTERNET SERVICES PROVIDERS CODES OF CONDUCT

	1. Existence of a code of conduct adopted by national Associations of ISPs	2. Association adopting the code of conduct	3. Scope of applicability of code of conduct	4. Existence of provisions concerning "illegal activity"	5. Existence of provisions on "notice and take down procedures"	6. Existence of provisions to regulate cooperation with law enforcement agencies and third parties
AUSTRIA	Yes	ISPA (http://www.ispa.at)	a) Service Providers b) Content Providers c) Access Providers d) Host providers e) Backbone providers Responsibilities are allocated according to the status of members (Art. 2).	Yes On discovery of publicly accessible, criminal content ("illegal content"), ISPA members will prevent access to the same using the technical and economic means at their disposal (Art. 4).	Yes Members are informed by the Austrian Internet Hotline and immediately block access to the content concerned. Where technically and economically feasible, they secure the relevant evidence for one calendar month (Art 4).	Yes (Art. 4)
BELGIUM	Yes	ISPA (http://www.ispa.be)	a) Service Providers (Art. 1)	Yes ISPs shall undertake in particular to fight against the presence of illegal or doubtful material on the Internet. They shall pay particular attention that the Internet is used legally (Art. 3).	Yes (Art. 3)	Yes Members must assist the authorities without delay, in every way possible and according to the means and resources available to them (Art. 3).
DENMARK	No	ISPA (http://www.ispa.de)	-	-	-	-
FINLAND	No	-	-	-	-	-

	1. Existence of a code of conduct adopted by national Associations of ISPs	2. Association adopting the code of conduct	3. Scope of applicability of code of conduct	4. Existence of provisions concerning "illegal activity"	5. Existence of provisions on "notice and take down procedures"	6. Existence of provisions to regulate cooperation with law enforcement agencies and third parties
FRANCE	Yes	AFA - Internet Service Providers Association (http://www.afa-france.com)	a) Service Providers b) Access providers c) Content providers d) Hosting providers e) Infrastructure providers (Introduction)	Yes (Art. II.2)	Yes	Yes (Art. I.2.4)
GERMANY	Yes	ECO - Association of the German Internet Economy (www.eco.de)	a) Service Providers b) Content providers c) Hosting providers d) Infrastructure providers (Art.2)	Yes References to the German law	Yes	Yes The complaints office can inform in each case authorities, also abroad, about the content of the complaint and the suspicion resulting in from it.
GREECE	No	-	-	-	-	-
IRELAND	Yes	ISPA (www.ispa.ie)	a) Service Providers b) Content providers	Yes	Yes Requests from Internet hotline for removal of specified potentially illegal content shall be deal with within a reasonable time (Art. 7).	Yes Cooperation with law enforcement through Internet hotline established by ISPA (Art. 7)
ITALY	Yes	AIIP (http://www.aiip.it)	a) Service Providers b) Access providers c) Content providers d) Hosting providers	Yes Obligations are set down on the protection of human dignity, minors and public order (Art. 6).	Yes	Yes The legal authorities must be informed of the existence of material of a potentially illicit nature which is accessible to the public (Art. 6).

	1. Existence of a code of conduct adopted by national Associations of ISPs	2. Association adopting the code of conduct	3. Scope of applicability of code of conduct	4. Existence of provisions concerning "illegal activity"	5. Existence of provisions on "notice and take down procedures"	6. Existence of provisions to regulate cooperation with law enforcement agencies and third parties
LUXEMBOURG	No	ISPA (http://dc.lux.com)	-	-	-	-
THE NETHERLANDS	Yes	NLIP (http://www.nlip.nl)	a) Service Providers	Yes General mention of cooperation in combating illegal activities (Art G.3)	Yes	Yes A report Centre is available and is recognised by the Government (Art. G.2).
PORTUGAL	No	ISPA (http://www.apritel.org)	-	-	-	-
SPAIN	No	AESPI (http://www.aespi.org)	-	-	-	-
SWEDEN	No	-	-	-	-	-
UNITED KINGDOM	Yes	ISPA (http://www.ispa.org.uk)	a) Service Providers	Yes Members shall ensure that services and promotional material do not contain anything which is in breach with UK law (Art. 2.2).	Yes Requests for removal are received from the IWF hotline (Art. 5)	Yes (Art. 5)

	<i>7. Existence of provisions on tools and services supplied to users to facilitate parental controls</i>	<i>8. Existence of rules on the management of complaints for breach of the code</i>	<i>9. Existence of sanctions for violations of the code of conduct</i>	<i>10. Existence of provisions regarding review and amendment of the code of conduct</i>	<i>11. Existence of provisions regarding data protection and privacy</i>
AUSTRIA	Yes Filtering and rating systems (Art. 6).	Yes Reports to be made in writing (e-mail, fax or letter) (Art. 8).	Yes From warning to termination of membership depending on seriousness of the case and frequency of the non-observance (Art. 8).	Yes Adjustment at regular intervals (Art. 8).	Yes (Art. 3).
BELGIUM	No	Yes Reports can be received directly by the concerned ISP (e-mail, fax or letter) (Art. 4).	Yes Exclusion for repeated non-compliance (Art. 4).	Yes Adjustment when remarks are made (Art. 8).	Yes (Art. 2).
DENMARK	-	-	-	-	-
FINLAND	-	-	-	-	-
FRANCE	Yes Filtering systems (Art. I.4)	Yes (Art. III)	Yes (Art. III)	No	Yes (Art. I.2.1)
GERMANY	Yes	Yes	Yes Members can be excluded from the membership.	No	Yes
GREECE	-	-	-	-	-
IRELAND	Yes Members must provide information to customers about the availability of software tools which may assist them in filtering content (Art. 5).	Yes A complaint analysis procedure should be started within 7 working days. A very detailed procedure follows (Art. 11).	Yes Variety of sanctions from suspension to expulsion (Art. 12).	Yes Review one year after code implementation, then periodic review (Art. 3.5)	Yes Members have to comply with Data Protection Act, 1988 (Art. 9)
ITALY	Yes Filtering methods and tools must be made available (Art. 6).	Yes Written complaints are received. A procedure of analysis of the complaint is started (Art. 13).	Yes From intimidation to formal admonition to be published on the site (Art. 13).	Yes Recommendations and amendments are analysed in order to implement and upgrade the code (Art. 4).	Yes (Art. 4)
LUXEMBOURG	-	-	-	-	-

	<i>7. Existence of provisions on tools and services supplied to users to facilitate parental controls</i>	<i>8. Existence of rules on the management of complaints for breach of the code</i>	<i>9. Existence of sanctions for violations of the code of conduct</i>	<i>10. Existence of provisions regarding review and amendment of the code of conduct</i>	<i>11. Existence of provisions regarding data protection and privacy</i>
THE NETHERLANDS	Yes (Art. II)	Yes Complaints must be forwarded via e-mail, fax, letter or telephone. Complaints are dealt with within 3 days, judgement within two weeks.	Yes From strict instructions, to temporary suspension, to cancellation of service (Art. K.9).	No	Yes (Art. G.2)
PORTUGAL	-	-	-	-	-
SPAIN	-	-	-	-	-
SWEDEN	-	-	-	-	-
UNITED KINGDOM	Yes Members should provide information to customer about the availability of tools that may assist them in filtering Internet content (Art. 7).	Yes Complaints have to be dealt with within 10 days. Then an ISPA complaints procedure is started (Art. 8.2 and 8.3)	Yes From a request to remedy the breach of the code, to suspension and expulsion (Art. 8.5)	Yes (Art. 9)	Yes Members shall comply with UK legislation on data protection (Art 4)

ANNEX 4

QUESTIONNAIRE ON THE EVALUATION OF ISPS' SELF REGULATION ACTION AGAINST CHILD PORNOGRAPHY ON THE INTERNET

A) CODES OF CONDUCT - GENERAL CHARACTERISTICS

1. According to your experience, how do you evaluate the adequacy of your code of conduct definition of illegal activities identifying behaviours on the Internet (1 = totally ineffective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Does your association provide its members with a hotline in order to report any child pornography material, which is distributed through them?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 3

2.1 How do you evaluate the usefulness of such a hotline facility in order to tackle child pornography (1 = totally ineffective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2.2 Please, quantify the number of reports received in years 2001 and 2002

2001 _____

2002 _____

3. If you have established any procedure to withdraw child pornography material which might be distributed exploiting your associates services, how do you evaluate its effectiveness (1= totally ineffective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. How do you evaluate the rules you have defined to manage complaints concerning breach of the code (1= totally inadequate, 2= scarcely adequate, 3= adequate and 4= very adequate)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Have you established any sanctions for the violation of the code of conduct?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 6.

5.1 Have you ever inflicted a sanction on your associates for a breach of the code of conduct?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

5.2 With regards the sanctions you have inflicted on your associates for breaches of the code of conduct, please specify the number of sanctions for each type:

Oral warning _____ n. _____
 Written warning _____ n. _____
 Public reprimand _____ n. _____
 Temporary suspension _____ n. _____
 Termination of the membership _____ n. _____

5.3 How do you evaluate the sanctions you impose in case of violation of the code of conduct (1= totally inadequate, 2= scarcely adequate, 3= adequate and 4= very adequate)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Have you ever updated your the code of conduct?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 7.

6.1 How do you evaluate the frequency of your code of conduct updates (1= totally inadequate, 2= scarcely adequate, 3= adequate and 4= very adequate)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B. PREVENTION AND CONTROL

7. According to your experience, how do you evaluate the usefulness of filtering systems to tackle child pornography on the Internet (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. How do you evaluate the usefulness of website content rating systems to tackle child pornography on the Internet (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9. How do you evaluate your associates own control systems for combating the production, processing, possession and distribution of child pornography material through the Internet (1= totally inadequate, 2= scarcely adequate, 3= adequate and 4= very adequate)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10. According to your association's code and/or national regulations, has an ISP the duty to clearly identify (i.e. name, addresses, etc) a customer when he/she signs an agreement to subscribe to ISP services such as email facilities or web page storage?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 11.

10.1 How do you evaluate the effectiveness of this provision as a means of reducing anonymity in the case of illegal conduct (1= completely useless, 2= quite useful, 3= useful and 4= very useful) ?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

11. If any measure exists in your country empowering competent authorities to order an ISP to provide subscriber information during an investigation in a child pornography case, how do you evaluate its usefulness (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

12. If an IPS's client has the duty to sign contractual provisions to ensure that illegal material is not exchanged/provided/shown on the Internet, how do you evaluate its usefulness (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. According to your national regulations, could an ISP be subject to criminal penalties due to a lack of monitoring of its subscribers' behaviours?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 14.

13.1 How do you evaluate the effectiveness of such a provision to tackle child pornography on the Internet(1= totally ineffective, 2= quite effective, 3= effective and 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

C. COOPERATION WITH LAW ENFORCEMENT AGENCIES

14. According to your national regulations, have ISPs a duty to advise competent authorities about child pornography material which is distributed through it?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

If the answer is NO, please, go to question 15

14.1 How do you evaluate the effectiveness of such a provision in order to tackle child pornography on the Internet (1= totally ineffective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

14.2 Please, quantify approximately the number of ISP reports to law enforcement in year 2002 and 2001

2001_____

2002_____

15. How do you evaluate the level of cooperation between law enforcement agencies and ISPs to tackle child pornography on the Internet (1= totally ineffective, 2= quite effective, 3= effective, 4= very effective)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

15.1 Please, quantify approximately the number of investigations, which were conducted by ISPs in cooperation with law enforcement agencies in years 2001 and 2002

2001_____

2002_____

16. If a measure exists in your country, which imposes a duty on Internet providers to retain *traffic-data* for law enforcement investigative purposes, how do you evaluate its usefulness to tackle child pornography on the Internet (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

17. If a measure exists in your country, which imposes a duty on Internet providers to retain *content-data* for law enforcement investigative purposes, how do you evaluate its usefulness to tackle child pornography on the Internet (1= completely useless, 2= quite useful, 3= useful and 4= very useful)?

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

18. Has a common platform been established between your association and law enforcement agencies to ease the cooperation when carrying out an investigation on child pornography on the Internet?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

18.1 If the answer to the previous question is No, do you think that such a common platform might be useful in order to tackle child pornography on the Internet?

YES	NO
<input type="checkbox"/>	<input type="checkbox"/>

18.2 If the answer to the previous question is No, please, explain your reasons briefly.

15.

ANNEXES REGARDING AREA OF INTERVENTION C (AWARENESS AND EDUCATIONAL FIELD)

ANNEX 1

QUESTIONNAIRE SENT TO GOVERNMENTS

This instrument is designed to map **awareness raising and educational initiatives** concerning child pornography on the Internet. To this end it addresses inputs, that is, policy formulation and concrete activities. It is not intended to assess the outputs or results of these activities. Your contribution will be part of a European Union funded study to assess awareness raising and education initiatives across the EU Member States. The results will be used to describe the pattern of initiatives within the EU, and will form the basis of a subsequent round of research intended to identify the most effective means of reducing the quantity of child pornography on the Internet.

This questionnaire is divided into two sections:

Section I "Political Context"

This section is intended to assess the government's commitment to implementing preventive measures against child pornography on the Internet, and specifically awareness and educational initiatives. To this end, it deals specifically with public policy and governmental reports, where these exist.

Section II "Awareness Campaigns and Education"

This deals with the concrete implementation of awareness campaigns and education initiatives. These initiatives may be trans-national, with a significant component in your country, national or sub-national. **Please note that by sub-national we refer to the level of government administration immediately below the central level.**

GENERAL COMMENTS

I. POLITICAL CONTEXT

1. Has the government of ... issued a report on the nature and scale of child pornography on the Internet?

- Yes
 No

- If yes, i) which of the following contributed to this report?

- Government ministries
 Other government bodies
 Non-governmental organisations
 Academic institutions
 Individual experts
 Internet industry
 Others (please specify)

ii) for whose use is the report intended?

- Unspecified
- Policy makers
- Law enforcement agencies & judiciary
- Professional in child-related fields
- Internet industry
- General public
- Others (please specify)

iii) does the report specifically address awareness raising and education initiatives?

- Yes
- No

- If yes, is the report available on a website? Please provide us with the website address

http://www.

Alternatively, could you send us a copy of this document or indicate from where we might obtain a copy?

2. Has the government adopted a National Plan of Action on the sexual exploitation of children (in the context of the Stockholm Congress, 1996)?

- Yes
- No

- If yes, does this National Plan of Action address child pornography on the Internet?

- Yes
- No

- If yes, does this National Plan of Action address education and awareness raising regarding child pornography on the Internet?

- Yes
- No

- If yes, i) please indicate the duration of this National Plan of Action?

- 1 to 3 years
- 4 to 5 years
- 6 to 10 years
- More than 10 years
- Not specified

ii) regarding education and awareness raising, which actors does the National Plan consider should be involved in promoting these activities?

- Central government
- Local government
- Parliamentarians
- Non-governmental organisations
- Law enforcement agencies & judiciary
- School teachers
- Welfare services
- Health services
- Internet industry
- General public
- Others (please specify)

iii) according to the National Plan, who should be the target of education and awareness campaigns?

- Children & young people
- Parents
- General public
- Law enforcement agencies & judiciary
- School teachers
- Welfare services
- Health services
- Internet industry
- Others (please specify)

iv) if the National Action Plan is available on Internet, please provide us with the website address

Alternatively, could you indicate from where we might obtain a copy?

3. Has the government of ... officially committed itself to the EU Action Plan for promoting the Safer Use of the Internet?

- Yes
- No

- If yes, how and when was this formal commitment made?

II. AWARENESS CAMPAIGNS AND EDUCATION

Regarding concrete activities:

4. Does the government provide financial support to any non-governmental initiatives for awareness raising or education?

- Yes
 No

- If yes, i) does the government

- Actively seek initiatives to fund
 Respond to funding requests on an ad hoc basis

ii) does the government make any assessment or evaluation of the result or outcomes of funded initiatives

- Yes
 No

5. If the government provides financial support, which ministry (or ministries) plays a key role?

- Communication
 Culture
 Education
 European Affairs
 Family and children affairs
 Health
 Interior
 Justice
 Social affairs
 Welfare
 Other (please specify)

6. Has the government of ... directly organised a national awareness campaign regarding child pornography on the Internet?

- Yes
 No

- If yes i) which government ministry was principally responsible for running this campaign?

ii) was this campaign principally directed at:

- Children & young people
- Parents
- General public
- School teachers
- Welfare services
- Health services
- Others (please specify)

iii) if there is a website for this campaign, please provide the address

If not, could you indicate where we might obtain this material

7. Have there been any significant sub-national (regional) awareness campaigns regarding child pornography on the Internet organised by local government?

- Yes
- No

- If yes, for each campaign please state which local government authority was responsible, who was the principle target of the campaign, and how long the campaign lasted. Please add website details where appropriate.

QUESTIONNAIRE SENT TO EXPERTS

This instrument is designed to map **awareness raising and educational initiatives** concerning child pornography on the Internet. To this end it addresses inputs, and is not intended to assess the outputs or results of these activities. Your contribution will be part of a European Union funded study to assess awareness raising and education initiatives across the EU Member States. The results will be used to describe the pattern of initiatives within the EU, and will form the basis of a subsequent round of research intended to identify the most effective means of reducing the quantity of child pornography on the Internet.

This questionnaire deals with the concrete implementation of awareness campaigns and education initiatives. These initiatives may be trans-national, with a significant component in your country, national or sub-national. **Please note that by sub-national we refer to the level of government administration immediately below the central level.**

GENERAL COMMENTS

1. Are any **NGOs** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the names of these organisations⁸:

- a)
- b)
- c)
- d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- a) target
period
- b) target
period
- c) target
period
- d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign

⁸ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

Other (cinema, radio, etc.) Please specify

iv) did the campaign receive financial support from central government?

a) b) c) d)

Yes, full support

Yes, partial support

No

Please add any other information relevant to this/these campaign, or other significant initiatives:

2. Are any **Internet Providers** involved in promoting education or awareness regarding child pornography on the Internet?

Yes

No

- If yes, i) please supply the names of these providers⁹:

a)

b)

c)

d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

a) target
period

b) target
period

c) target
period

d) target
period

iii) is/was this education and awareness raising carried out through

a) b) c) d)

Website based in ...

a) www.

b) www.

c) www.

d) www.

Printed leaflets or brochures

Campaign on daytime television

Campaign on evening television

National newspapers campaign

Local newspaper campaign

Other (cinema, radio, etc.) Please specify

⁹ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
 Yes, full support
 Yes, partial support
 No

Please add any other information relevant to this/these campaign, or other significant initiatives:

3. Are any **Education Authorities** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the names of these authorities¹⁰:

- a)
b)
c)
d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- a) target
period
b) target
period
c) target
period
d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign
 Other (cinema, radio, etc.) Please specify

¹⁰ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
 Yes, full support
 Yes, partial support
 No

Please add any other information relevant to this/these campaign, or other significant initiatives:

4. Are any **Welfare Services** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the names of these welfare services¹¹:

- a)
b)
c)
d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- a) target
period
b) target
period
c) target
period
d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign
 Other (cinema, radio, etc.) Please specify

¹¹ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
 Yes, full support
 Yes, partial support
 No

Please add any other information relevant to this/these campaign, or other significant initiatives:

5. Are any **Law Enforcement Agencies** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the names of these agencies¹²:

- a)
b)
c)
d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- (a) target
period
(b) target
period
(c) target
period
(d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign
 Other (cinema, radio, etc.) Please specify

¹² If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
 Yes, full support
 Yes, partial support
 No

Please add any other information relevant to this/these campaign, or other significant initiatives:

6. Are the **Media** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the name of the media group and the type of medium (eg newspaper, tv)¹³:

- a)
b)
c)
d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- a) target
period
b) target
period
c) target
period
d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign
 Other (cinema, radio, etc.) Please specify

¹³ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
 Yes, full support
 Yes, partial support
 No

Please add any other information relevant to this/these campaign, or other significant initiatives:

7. Are any **Other Bodies** involved in promoting education or awareness regarding child pornography on the Internet?

- Yes
 No

- If yes, i) please supply the names of these bodies¹⁴:

- a)
b)
c)
d)

ii) who is/was the target of this education and awareness raising and what is/was the time period of the campaign?

- a) target
period
b) target
period
c) target
period
d) target
period

iii) is/was this education and awareness raising carried out through

- a) b) c) d)
 Website based in ...
a) www.
b) www.
c) www.
d) www.
 Printed leaflets or brochures
 Campaign on daytime television
 Campaign on evening television
 National newspapers campaign
 Local newspaper campaign
 Other (cinema, radio, etc.) Please specify

¹⁴ If you know of more than 4, please indicate additional significant initiatives under "any other information" at the end of this question.

iv) did the campaign receive financial support from central government?

- a) b) c) d)
- Yes, full support
- Yes, partial support
- No

Please add any other information relevant to this/these campaign, or other significant initiatives:

8. Is there a national committee with a mandate to coordinate the education and awareness initiatives detailed in questions 1 to 7?

- YES
- NO

9. To your knowledge, have national awareness initiatives or specific materials been aimed at children and young people in school?

- Yes
- No

- If yes, can you provide us with details of these, or supply a website address

10. To your knowledge, have sub-national (regional) awareness initiatives or specific materials been aimed at children and young people in school?

- Yes
- No

- If yes, can you provide us with details of these, or supply website addresses

11. Have schools taken steps to develop and promote educational material regarding child pornography on the Internet in a nationally coordinated initiative?

- Primary schools
- Secondary schools

- If yes, can you provide us with details of these, or supply a website address

12. Have any schools taken coordinated steps to develop and promote educational material regarding child pornography on the Internet in sub-national initiatives?

- Primary schools
- Secondary schools

- If yes, can you provide us with details of these, or supply website addresses

13. Have any national-level seminars or congresses regarding child pornography on the Internet been organised in your country?

- Yes
 No

- If yes, for each seminar or congress please state who organised the event, when it was held and at whom it was directed (audience)
Please also provide website addresses where appropriate

14. With respect to child pornography on the Internet, are you aware of national initiatives regarding the training of:

- School teachers
by whom was this training carried out?
- Welfare services
by whom was this training carried out?
- Health Services
by whom was this training carried out?
- Law enforcement agencies
by whom was this training carried out?
- Judicial authorities
by whom was this training carried out?
- Public officials
by whom was this training carried out?
- Others (journalists, etc.) please specify

15. With respect to child pornography on the Internet, are you aware of sub-national (regional) initiatives regarding the training of:

- School teachers
by whom was this training carried out?
- Welfare services
by whom was this training carried out?
- Health Services
by whom was this training carried out?
- Law enforcement agencies
by whom was this training carried out?
- Judicial authorities
by whom was this training carried out?
- Public officials
by whom was this training carried out?
- Others (journalists, etc.) please specify

ANNEX 2

SYNOPTIC TABLE REGARDING GOVERNMENT ADHERENCE TO EU GUIDELINES, JUNE 2003

Table 1 of 3

Country/Actions	General guideline	
	<i>Guideline 1.1</i>	<i>Guideline 1.2</i>
	Existence of a report on the subject	Official Commitment of the Government to the EU Action plan
Austria	1	1
Belgium		
Danemark	1	1
Finland	1	1
France	1	1
Germany	1	1
Greece		
Ireland	1	1
Italy	1	/
Luxembourg	/	1
Netherlands	/	/
Portugal	/	/
Spain		
Sweden	0	1
UK	0	1

Table 2 of 3

Thematic field: awareness initiatives						
Country/Actions	Guideline 2.1	Guideline 2.2	Guideline3.1	Guideline3.2	Guideline3.3	Guideline3.4
	Existence of financial support by the government	Existence of any national-level seminars or congresses	Existence of a national campaign regarding child pornography on the Internet directed at			
			Children and Young people	Parents	General Public	School teachers
Austria	1	1	0	0	0	0
Belgium		1				
Danemark	1	1	0	0	0	0
Finland	1	1				
France	/	1				
Germany	1		1	1	1	1
Greece		0				
Ireland	/	1			1	
Italy	/	1				
Luxembourg	/					
Netherlands	/	1				
Portugal	/	0				
Spain		0				
Sweden	1	1				
UK	0	1	1	1	0	1

Table 3 of 3

Country/Actions	Thematic field: education initiatives										Thematic field: Coopera
	Guideline 4.1	Guideline 4.2	Guideline 4.3	Guideline 4.4	Guideline 4.5	Guideline 4.6	Guideline 4.7	Guideline 4.8	Guideline 4.9	Guideline 4.10	Guideline 5
	Existence of national initiatives regarding training of:					Existence of regional initiatives regarding the training					Regular meeting of competent
	Children	School teachers	Law enforcement	Public officials	Others	Children	School teachers	Law enforcement	Public officials	Others	authorities specialising in combating child pornography on the
Austria	1					1	1				/
Belgium	1	0	1	0	0	1	0	0	0	0	1
Danemark											
Finland	1	1	1	1	1	0	0	0	0	0	0
France	1					1					0
Germany											1
Greece	0					0					0
Ireland	1	1	0	0	0	/	0	0	0	0	1
Italy	1					1					0
Luxembourg											
Netherlands	1	/	/	/	/	1	1	0	0	1	1
Portugal	0	1	1	1	1	0	1	0	0	0	0
Spain	1	1	1	1	0	0	0	0	0	0	0
Sweden	1	1				1	1				0
UK	1	1	1	0	1	1	1	1	1	0	1

Table 2 of 2

Thematic field: awareness and education initiatives														
Guideline 4. Guideline 4. Guideline 4. Guideline 4. Guideline 5. Guideline 5. Guideline 5. Guideline 5. Guideline 7. Guideline 7. Guideline 7. Guideline 7.														
Country/Actions	Existence of Law Enforcement Aqs involved in				Existence of Media involved in promoting a				Existence of		Existence of Other bodies involved in promo			
	Children and Parents people	General Public	School teachers	Young people	Children and Parents Young people	General Public	School teachers	European Projects	Children and Parents Young people	General Public	School teachers			
Austria	0	0	0	0	1	1	1	0	1	0	1	0	1	
Belgium	1	1	0	0	1	0	0	0	1	1	1	1	1	
Danemark	1	1	0	1	1	1	1	1	1	0	0	1	1	
Finland	0	0	0	0	/	/	/	/	1	0	1	0	1	
France			1				1		1	1	0	0	1	
Germany	1	1	1	0			1		1	1	1	1		
Greece	/	/	/	/	1	1	1	1	1	0	1	0	1	
Ireland	/	/	/	/	/	/	/	/	1	1	1	1	1	
Italy			1				1		1	1	1	1	1	
Luxembourg	0	0	1	0										
Netherlands			1				1		1	0	1	1	1	
Portugal	0	0	0	0	0	0	0	0	1	0	0	1	0	
Spain	1	1	1	0	0	0	0	0	1	1	1	1	1	
Sweden	1	0	1	0					1	0	1	0	1	
UK			1		0	1	0	0	1	1	1	1	1	

ANNEX 3

SYNOPTIC TABLE REGARDING THE EXISTENCE OF EDUCATION AUTHORITIES INVOLVED IN PROMOTING EDUCATION OR/AND AWARENESS INITIATIVES

COUNTRY/TARGET	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 3.1	Guideline 3.2	Guideline 3.3	Guideline 3.4	Guideline 3.5	Guideline 3.6
Austria	<p>Yes</p> <p>Institut für Gewalverzicht Beratungsgesellschaft m.b. H (National partner SUI European Project) About 300 schools are using the "websense" software system. Preparation of information papers on a range of Safer Internet topics: German text to different age groups, 6-10; 10-14 and 15-18 year-old pupils and children no longer in schooling, similar material but aimed at teachers adult educators, parents, general users, seminars in schools and adult education work-shops</p> <p>No Landesakademie Institute (National Partner for the CISA European project)</p> <p>They conducted a study with children, teens and their parents in Lower Austria. The results were striking. They found that youngsters seem to be far more competent than their parents.</p>				No	No
Belgium	<p>Yes</p> <p>Large awareness-raising campaign launched on December 2002 by the Ministry of Justice, the Ministry for Education and training, Child Focus, the federal police computer crime unit and the media VT4. The campaign materials are/ safety guide for teachers, posters for schools, website, boomerangs cards, etc</p>				No	No
Denmark	<p>Yes</p> <p>Project "ror nettet" "touch the web" producing comprehensive materials on safety issues, the objectives are to render children responsible users</p> <p>The Ministry of Education has, for this purpose, joined forces with UNI-C, the Danish Centre for Education and Research, and with DR, one of the two Danish national television channels.</p> <p>A number of television programmes will be an important element in promoting safe Internet use. Other elements will include websites for different target groups, printed educational material and internet games for children.</p> <p>Target groups are not only children but the whole range of grown-ups who are involved with children's education and upbringing :parents and grandparents, teachers, school boards, etc...</p>					
Finland	Yes	Yes	Yes	Yes	No	No

Country/Target	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 3.1	Guideline 3.2	Guideline 3.3	Guideline 3.4	Guideline 3.5	Guideline 3.6
France	Yes CLEMI (National Centre of Pedagogical Documentation of the Education ministry) is participating to the Educaunet European project that aims to help children develop an autonomous and responsible attitude towards their use of the Internet	No	No	Yes Académie de Grenoble is participating to the European Dotsafe project Is providing European schoolteachers with effective means for safe Internet use to lay down the foundations for large-scale actions focused on schools		
Germany	The European Commission project SIFKAL(Safer Internet for Knowing and Living) supported by the German Institute for Law & Informatics is building up an international network of examples of how to use the Internet, without making use of technical and restrictive norms. The project aims is to create a “permanent observatory” for Safer Internet (OFSI), for the diffusion of information, experiences, ideas, documents, links and actions”.					
Greece	Yes	Yes	No	Yes	Yes	Yes
Ireland	Yes Active in two European projects, namely DoSafe and ONCE IN IRELAND, THERE ARE FOURTEEN SCHOOLS INVOLVED IN THE ONCE PROJECT. A CORE ELEMENT OF THE ONCE PROJECT IS THE DELIVERY OF WORKSHOPS TO STUDENTS, TEACHERS AND PARENTS IN THE PROJECT SCHOOLS, ON BOTH TECHNICAL AND NON-TECHNICAL ISSUES RELATING TO INTERNET SAFETY. AS PART OF THE ONCE PROJECT, THE “FOR KIDS BY KIDS ONLINE” WEBSITE (WWW.FKBKO.NE) HAS BEEN ESTABLISHED AS A FUN INTERACTIVE SITE FOR STUDENTS OF ALL AGES. One of the aims of the Internet Safety team at the NCTE is to educate children so they are able to protect themselves from these online dangers.					

Country/Target	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 3.1	Guideline 3.2	Guideline 3.3	Guideline 3.4	Guideline 3.5	Guideline 3.6
Italy	<p style="text-align: center;">Don't know</p> <p>But the project Webscuola is part of the FRIENDLY INTERNET European project which aims at achieving a larger and safer use of the net by promoting the role of parents, teachers and social assistants. The pilot phase will involve secondary and high schools in Italy. The awareness campaign will be based on information didactic materials, meetings in schools and through the special site "web-scuola".</p>					
Luxemburg						
Netherlands	<p style="text-align: center;">Yes</p> <p>Government and private sector together have started at the end of the year 2001 under the name www.surfopsafe.nl an awareness campaign on safe surfing</p> <p>Several partners work together, like governments (ministry of education, ministry of justice, ministry of transport/communication), libraries, associations of internet users and the private sector</p> <p>Kennsinet is a safe portal and the organisations behind it are the Ministry of Education, culture and Science. It offers connections to institutions of vocational training and adult education, teacher training institutes, primary schools and secondary schools.</p> <p>As part of the European Learning environment project, one-day conference for Dutch teachers was organised: it focused on the different approaches of internationalisation.</p>				No	No
Portugal	<p style="text-align: center;">Yes</p> <p>A children's portal provides Internet security information and is linked, among others, to the European Schoolnet (IAP DotSafe) and EUN CLE projects and different Portuguese ministries such as the Ministry of Education, Ministry for Science and Technology and the Ministry of Culture.</p> <p>A Portuguese website (www.pedofilia.web.pt) provides information for parents and teachers and how to protect children.</p>				No	No
Spain	No	No	No	No	No	No
Sweden	<p style="text-align: center;">Yes</p> <p>Part of Schoolnet Dotsafe European project</p>	No	No	<p style="text-align: center;">Yes</p> <p>DotSafe provides European teachers with effective means for Safe Internet</p>	No	No
UK	<p style="text-align: center;">Don't know exactly</p> <p>Education authorities run internal training sessions for their staff in many parts of the UK, but it is likely that child pornography would only be mentioned in passing. The content and coverage of those sessions is mixed and many staff will not have attended one. Updating sessions for staff seem to be rare.</p> <p>The UK Department for Education and Skills regularly updates its advice to schools and local authorities, called "Superhighway Safety"</p> <p>The Scottish Executive Education Department produced "Clickthinking", a similar set of material that provides advice to local authorities and schools about setting up of suitable systems and politics</p>					

SYNOPTIC TABLE REGARDING THE EXISTENCE OF EXISTENCE OF INTERNET PROVIDERS INVOLVED IN PROMOTING EDUCATION OR/AND AWARENESS INITIATIVES

Country/Target	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 2.1	Guideline 2.2	Guideline 2.3	Guideline 2.4	Guideline 2.5	Guideline 2.6
Austria	Yes Cyber Tron Regional project, by supplying 8 h free family surfing for family cars members in Lower Austria plus supplying information on safer use o the Internet			No	No	No
Belgium	Yes Active in the fight against harmful and illegal online contents. Agreement that regularises the collaboration between the ISPA, the Ministry of Justice, the Ministry of Telecommunications and the Federal Computer Crime Unit			No	No	No
Denmark	No	No	No	No but Lectures at schools The Danish IT industry association calls on school teachers to contact members of the association who will then give lectures	No	No
Finland						
France	Yes Creation of a new website – www.pointdecontact.org The advice centres on a family charter and a code of “good practices” to enable dialogue between parents and children. This guide will soon be offered automatically through Internet kits provided by members of AFA			No	No	No
Germany	Don' t know	Don' t know	Don' t know	Don' t know	Don' t know	Don' t know
Greece						

Country/Target	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 2.1	Guideline 2.2	Guideline 2.3	Guideline 2.4	Guideline 2.5	Guideline 2.6
Ireland	No	No	Yes	No	No	No
Italy	No	No	Yes Stop-it.org was launched on November 2002 financed by the EU, it is supported by a number of child and consumer protection organisations (ECPAT, Movimento consumatori, Consiglio Nazionale degli Utenti, ARCI) and Internet service providers (Tiscali, AIP) Raising awareness id one of the main objective	No	No	No
Luxemburg						
Netherlands	Yes The activities of the Safe Internet Foundation (SIF) are directed at the Internet users in general and the business sector and privacy users are the biggest targets There are close connections among the projects and initiatives exchange, the service is coordinated by NLIP and all the different actors of the association work closely at national or European level					
Portugal						
Spain	Yes	Yes	Yes	No	No	No
Sweden	Yes	No	Yes	No	No	No
UK	Don't know exactly because In the UK there is a growing number of websites to inform internet users of all ages about potential dangers and how to surf safely. On these websites, there is plenty of good advice in designs that reflect the target group : interactive and colourful websites for children and teenagers, informative websites for parents, teachers and responsible adults.					

SYNOPTIC TABLE REGARDING THE EXISTENCE OF EXISTENCE OF LAW ENFORCEMENT AGENCIES INVOLVED IN PROMOTING EDUCATION OR/AND AWARENESS INITIATIVES

Country/Target	Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	Guideline 4.1	Guideline 4.2	Guideline 4.3	Guideline 4.4	Guideline 4.5	Guideline 4.6
Austria	No	No	No	No	No	No
Belgium	<p align="center">Yes</p> <p><i>Large awareness-raising campaign launched on December 2002 by the Ministry of Justice, the Ministry for Education and training, Child Focus, the federal police computer crime unit and the media VT4. The campaign materials are/ safety guide for teachers, posters for schools, website, boomerangs cards, etc</i></p>				No	No
Denmark	<p align="center">Yes</p> <p>In November 2001, poster accompanied the awareness leaflet on chat safety and safer use of Internet. Both were part of a campaign introduced by the Danish Crime Prevention Council and Red Barnet</p>		No	Yes	No	No
Finland	No	No	No	No	No	No
France			<p align="center">Yes</p> <p>Official website for reporting illicit websites and received information was launched on 9 November 2001. It is a joint initiative from various French ministries allowing people to report illicit content directly to OCLCTIC(Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication)</p>			
Germany	<p align="center">Yes</p> <p>The Federal Police Department (German Bundeskriminalamt) is very much aware of the dangers that comes with the Internet Installation of a Hotline and has installed a hotline to report illegal content</p>			No	No	No
Greece	Don't know	Don't know	Don't know	Don't know	Don't know	Don't know
Ireland	Don't know	Don't know	Don't know	Don't know	Don't know	Don't know
Italy			Yes			
Luxemburg	No	No	Yes	No	No	No
Netherlands			<p align="center">Yes</p> <p>Existence of a website: www.justitie.nl</p>			
Portugal	No	No	No	No	No	No
Spain	Yes	Yes	Yes	No	No	No
Sweden	Yes	No	Yes	No	No	No
UK			<p align="center">Yes</p> <p>Existence of the Internet crime forum Northumbria Police: local initiative with leaflet, Merseyside police: local initiative with Mousemat</p>			

SYNOPTIC TABLE REGARDING THE EXISTENCE OF NGOS INVOLVED IN PROMOTING EDUCATION OR/AND AWARENESS INITIATIVES

Country/Target	Children and Young people	Parents	General Public	School teachers	Welfare Services	Health Services
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 1.4	Guideline 1.5	Guideline 1.6
Austria	<p>Yes</p> <p>Education and awareness campaign through of: regional magazines for families, parents evenings with parents organisations, schools, kindergarten, national radio special programmes on children and computer, articles in special interest magazines, mothers courses, children holiday programme in youth centres, libraries, internet cafes, with board games, best websites for children, cyber spider surf card, etc</p> <p>All of these initiatives are of a regional/local character although in cooperation with the Internet Action Plan and the project CISA</p> <p>Webprize of the Region of Lower Austria within a project of media education and the internet</p>	Yes	No	Yes	No	No
Belgium	<p>Yes</p> <p>Large awareness-raising campaign launched on December 2002 by the Ministry of Justice, the Ministry for Education and training, Child Focus, the federal police computer crime unit and the media VT4. The campaign materials are/ safety guide for teachers, posters for schools, website, boomerangs cards, etc</p>				No	No
Denmark			<p>Yes</p> <p>In 1997, Red Barnet (Save the Children Denmark) brought the sexual abuse and exploitation of children through child pornography on the Internet to the attention of Danish people</p> <p>The children's rights organisation launched a hotline against child pornography in 1998</p> <p>This activity has undergone major development since Red Barnet joined INHOPE in 2001</p>			
Finland	<p>Yes</p> <p>There have been so many activities in this area. For example, in 1997, the Mannerheim League had launched a specific Internet safety Awareness programme with some support from Central Government.</p> <p>Save the children campaign begins from July 2002 onwards. Not all plans have been finalised. It might well be that TV will be used as one of the campaign tools in the future. Campaigns in newspapers and other media but mainly through interviews and programmes. Consultation of public</p>				No	No

Country/Target	Children and Young people	Parents	General Public	School teachers	Welfare Services	Health Services
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 1.4	Guideline 1.5	Guideline 1.6
France	Yes	Yes	Yes	Yes	Yes	Yes
Germany	Yes Site www.dksb.de that offers assistance to parents, teachers and others responsible and created by the Association for children safety		No	Yes	No	No
Greece	Yes Mainly via European Projects (IAP) : CISA, ONCE, Safeborders. These multipartner European projects are using a wide scope of campaigning means (indicative printed material, website, CD-Rom, Television and Radio broadcasts, advertising banners on the WWW, articles in newspapers-magazines, Info-Kiosks at trade exhibitions or conferences, training seminars Implementation of 20 complete internet seminars as well as more than thirty presentations up till now. The seminars were organised in cooperation with schools of the primary and secondary education, unions of parents and guardians, Greek municipalities, the Bureau of secondary education, association of teachers as well as with other citizen groups.					No
Ireland			Yes			

Country/Target	Children and Young people	Parents	General Public	School teachers	Welfare Services	Health Services
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 1.4	Guideline 1.5	Guideline 1.6
Italy	<p>Yes</p> <p>The project is a general awareness campaign on safer use of Internet. For this, the project is in touch with parents, internet providers, NGOs, education authorities, ICT industries</p> <p>Cooperation with Spanish partners via European projects: creation of the website "Capitannet", brochure and informative CD-Rom which will be distributed through specialised shops and/or during important popular events such as the cinema, theatre, concerts</p> <p>Recently, new websites have been born with the same focus of supporting families in providing internet connections free of any pornography or violence access</p> <p>Stop-it.org was launched on November 2002, financed by the EU, it is supported by a number of child and consumer protection organisations (ECPAT, Movimento consumatori, Consiglio Nazionale degli Utenti, ARCI) and Internet service providers (Tiscali, AIP) Raising awareness is one of the main objectives</p>				No	No
Luxemburg						
Netherlands	<p>Yes</p> <p>In 1999, Meldpunt and ECAPT-NL started the SurfSafe campaign (www.surfsafe.nl) for children, youth, parents, educators with tips on how to surf safely</p> <p>The goal of the SurfSafe campaign is to make children and youth and educators aware of how to use the internet safely. Meldpunt is funded by the Dutch Ministry of Justice and is associated to the INHOPE association with the Dutch special police unit on child pornography on the Internet</p> <p>It was thought to be better to concentrate on campaigning for a safer surfing attitude, and it was decided not to use the word sexual exploitation or child pornography</p>					
Portugal						
Spain	<p>Yes</p> <p>Internet campaign launched by the Asociación de Internautas (one of Spain's Internet users associations)</p>			No	No	No
Sweden	<p>Yes</p> <p>The "Reference Group", formed by Rädda Barnen, BRIS, a prominent Swedish organisation for the protection of children's rights in society, ECPAT, the Swedish police and three of Sweden's largest Internet Providers, is dealing with spreading and exchanging up-to-date information about problems associated with child pornography.</p>			No	No	No
UK	<p>Yes</p> <p>A broader internet safety awareness campaign, aimed at teachers and parents, part funded by EC Safer Internet Action Plan, with partners in Scotland, Iceland, Netherlands and Spain</p> <p>Underprivileged children in the London borough of Newham are being trained during a six-week training course to teach other teenagers in Internet safety (January 2002)-non-profit-making organisation Cyberangels</p> <p>The NSPCC (National Society for the Prevention of Cruelty to children) is a charity specialising in child protection which offers a helpline for children, available in multiple languages (e.g. Welsh, Hindi, Urdu, Bengali etc) for problems that they might encounter in real life and on the Internet. There is also a section on Internet safety, including its NetSmart Rules.</p> <p>Childnet has realised the Net Benefit Schools programme</p>				No	No

SYNOPTIC TABLE REGARDING THE EXISTENCE OF OTHER ACTORS INVOLVED IN PROMOTING EDUCATION OR/AND AWARENESS INITIATIVES

Country/ Target			Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	National Projects	European Projects						
	Guideline 5.1	Guideline 5.2	Guideline 5.3	Guideline 5.4	Guideline 5.5	Guideline 5.6	Guideline 5.7	Guideline 5.8
Austria	No	Yes	Yes	Yes	No	Yes	No	No
Belgium	Yes	Yes	Yes	No	Yes	No	No	No
Denmark	Don't know	Yes	No	No	Yes	No	No	No
Finland	No	Yes	No	Yes	No	Yes	No	No
France	Don't know	Yes	<p align="center">Yes</p> <p>Participation of the Institut National des consommateurs to the European Project "Consumer Internet Safety Awareness" which produces and delivers Internet safety information. It promotes positive experience of the Net through the testing of children's sites and publishing the best examples, encouraging family organisations to use the resources in their own countries to continue to spread of the educational material.</p> <p align="center">Website of the CNIL(Commission nationale de l'informatique et des libertés)</p>				No	No
Germany	Yes	Yes	<p align="center">Yes</p> <p>Bertelsman Foundation (national partner for the SIFKAL European project). The Foundation is developing a non-commercial, non-profit platform where children parents and educational staff can inform themselves about a safer and creative use of the Internet. Publication on self-regulating systems. It deals with the security of young Internet users, while maintaining freedom of information exchange on the Internet. Website www.Internet-abc.de</p> <p>October 2000: Identification of best practices Workshop (Bertelsman Foundation): best-practices models in German, British, Norwegian and American schools and to develop a manual on the responsible use of the Internet at German schools</p> <p>Webguide "multikids" assists children in surfing the Internet, developed by a group of students of the Stuttgart University of Media studies (500 links tested for their "child-friendliness")</p>					
Greece	Yes	Yes	No	Yes	No	Yes	No	No
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Italy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Luxemburg								

Country/ Target			Children and Young people	Parents	General Public	School Teachers	Welfare Services	Health Services
	National Projects	European Projects						
	Guideline 5.1	Guideline 5.2	Guideline 5.3	Guideline 5.4	Guideline 5.5	Guideline 5.6	Guideline 5.7	Guideline 5.8
Netherlands	No	Yes	Yes Foundation Safer Internet (SIF)–The website is a central information about online issues and news. The website is managed by SIF who are also present online and offer a regularly updated site with news, tips and further information on surfing concern. SIF supports the awareness campaign by offering two courses. One course, namely “My child and the Internet” has been developed to train library personnel to teach parents throughout the country about the Internet and how to use it.				No	No
Portugal	Don't know	Yes	Yes Portugal is Partner of the IAP-funded CISA project.				No	No
Spain	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Sweden		Yes	No	Yes	No	Yes	No	No
UK	Yes	Yes	Yes The Internet Watch Foundation hotline helps adults and children when they come across illegal and harmful content. The IWF works closely with the Internet Service Providers and local police forces, and any reports of illegal content in newsgroups and UK websites that are made to it are checked out and passed to the relevant police force. KidSmart roadshow – touring over 20 cities across the UK and the KidSmart Website					

SYNOPTIC TABLE REGARDING THE COMMITMENT OF THE GOVERNMENT TO THE EU ACTION PLAN FOR SAFER USE OF INTERNET

Country/Actions	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
Austria	Yes	<p>Yes</p> <p>National Report available at the Federal Ministry of Interior</p> <p>The NÖ Landesakademie Institute in Austria belongs to the Consumer Internet Safety Awareness (CISA), project funded under the European Commission's Safer Internet Action Plan (IAP). They conducted a study with children, teens and their parents in Lower Austria</p>	<p>Yes</p> <p>Resolution of the Council of Ministers for a "Plan of action against Child abuse and against Child pornography in the Internet"</p> <p>Resolution of the national E-156-NR 18 GD</p> <p>Resolution of the Council of Ministers against violence in society, domestic violence, and violence towards women and violence in the media</p>	Yes	Yes	No
Belgium		<p>No but</p> <p>Study undertaken by the Facultés Universitaires Notre-Dame de la Paix in Namur from September 2001 to April 2002</p>	Yes		Yes	<p>Yes, partly</p> <p><i>Government of the French-speaking community, in cooperation with Educaunet gave the green light to "Cliquer futé" in February 2003</i></p> <p><i>Target: children aged 6 to 12 years old, media kit package for parents, educators and teachers</i></p>

Country/Actions	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
Denmark	Yes	<p>Yes</p> <p>Report regarding the strengthened efforts to fight sexual exploitation, adopted by the Government, available on the home page of the Ministry of Social Affairs</p> <p>No Report on the scale of the problem. However, the Internet Support Unit at The National Commissioner of Police has drafted a report on a strengthened effort to fight "cyber crimes". This report contains statistics on received reports on child pornography on the Internet.</p> <p>In 2001 the Unit received approximately 1900 reports. The report has not been published.</p>	<p>Yes</p> <p>After the Second World Congress against CSEC (Yokohama 2001), the Minister of Justice has initiated consultations with different authorities and NGO's in order to exchange ideas and viewpoints on what future action can be taken in the fight against sexual exploitation of children, including child pornography.</p>	Yes	Yes	Yes
Finland	Yes	<p>Yes</p> <p><i>The study, assigned by the Finnish Ministry of Transport and Communication, examines the extent of harmful content on the Internet and how the Finnish authorities should react to it. The report particularly focuses on the consequences of rapidly changing technology. It maintains that not all the problems brought about by technology can be solved through it. Other means are needed. At the same time legislation has problems to meet the Information Society's challenges. The study concludes that prevention requires fast actions which re-organise various communities and the whole society. www. mintc.fi/publications</i></p>	<p>Yes</p> <p><i>As a next step to the study, the Finnish Ministry of Transport and Communications has started, in co-operation with TIEKE Finnish Information Society Development Centre, a project which aims to develop a Finnish self-regulatory system as part of the European Union's Safe Internet Action Plan.</i></p>	Yes	Yes	

COUNTRY/ACTIONS	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
France	Yes	<p>Don't know but Internet users are frequently confronted by harmful and illegal content while surfing the Net.</p> <p>In 2001, France created the Internet Rights Forum</p> <p>In March 2003, the government is weighting the creation of an Internet Higher Council with "civil society of Internet users", experts</p> <p>In 2003, two missions "Internet and the family" and "Internet in school" have been launched by the French Education Minister and Minister of family</p>	<p>Yes</p> <p>On 5 September 2001, the Government set up the families'online web-site, "familles en ligne": www.social.gouv.fr/famille-enfance/fam_lign/. This website explains the main benefits and risks of using the Internet and provides advice for parents and children on how to use the Internet without danger.</p> <p>An official website for reporting illicit websites www.Internet-mineurs.gouv.fr was created in November 2001. The website is housing all useful information on the laws and regulations regarding the protection of children in France.</p> <p>There are also many institutions that can help and give advice to people, mainly children and parents, such as www.defenseuredesenfants.fr, www.droitsdesjeunes.gouv.fr</p>	Don't know	Yes Rencontres du Net (Mars, 2002) organised by the Ministry of the employment	
Germany	Yes But done by the Foundation Bertelsman (2001)	No	<p>Yes</p> <p>A German initiative is the German Ministry for Economy and Technology and the Ministry for Internal Relations' website www.sicherheit-im-internet.de, with general information about Internet security. It contains a special section for pupils and students, with information about the dangers of Internet use and how they can protect themselves.</p>	Yes		Yes

Country/Actions	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
Greece	<p>No But</p> <p>Survey carried out by E.KA.TO, along with its European partners, Results : the safer Internet message was not getting through. In Greece, 864 children were surveyed with some interesting results.</p> <p>It showed that 98% of children have never been informed or have never heard about any guidelines and advice concerning the possible dangers of the Internet.</p>				No	
Ireland	<p>A 1998 Government report on the Illegal and Harmful Use of the Internet looked at issues surrounding the illegal and harmful use of the Internet. It recommended a system of self-regulation by service providers to tackle the problem and the setting up of an Internet Advisory Board. http://iab.ie/Publications/Reports</p>	<p>Research carried out by the Irish Information Society Commission in October 2000 showed that 95% believe that all school-children will be using computers as part of their education within the next ten years. Therefore in October 2001, the IAB launched a number of Internet Safety Initiatives designed to improve Internet safety.</p>	<p>Yes</p> <p>Included in its recommendations was the setting up of an Internet Advisory Board (IAB). In October 2001 the IAB launched a number of Internet Safety Initiatives. The Government is committed to taking all possible steps to minimise the dangers while at the same time productively exploiting the full resources of the Internet.</p>	Don't know	Yes	Yes

Country/Actions	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
Italy	Yes According to research commissioned by the Italian Ministry of Communications in February 2001, the typical Internet user seems to be young, male and educated. However, the number of children connecting to the Internet in Italy is growing fast and one in five has been the object of sexual proposals.	Don't know	Yes	Don't know	No	Yes Presentation of "Ciclope" in 2002 National Observatory to collect paedophile data, promotion of informative campaign telephone number for national aid
Luxembourg	Don't know	Don't know	Yes Launching of the website www.luxemburg.lu	Don't know		
Netherlands	Don't know	Don't know But In 2000 a booklet called 'Child pornography, the state of affairs' has been produced by GVAK to train police officers (and others who might encounter child pornography in their work) on all aspects of child pornography'.	The Dutch National Action Plan against Sexual child abuse, that includes child pornography as been presented to the Dutch parliament on 15 May 2000. A project team has been formed for the monitoring and implementation of this plan. The ministry of justice is leading, but it's the joint responsibility of all relevant ministries.	For its part, the Dutch Ministry of Justice is funding Surfopsafe.	Yes	Yes In July 2001, the Dutch Ministries of Economic Affairs and Transport, public works and Water Management, including different private organisations and companies has started an ongoing awareness campaign on how to use the Internet safely, especially in schools, together with the private sector. www.surfopsafe.nl

Country/Actions	Report on the nature and the scale of child pornography	Report addressing awareness campaigns and education initiatives	Official commitment of the Government to the EU Action Plan for the Safer use of Internet	Financial supports provided by the Government to NGOs	National level seminars or congresses	Existence of national awareness campaigns organised by the government
	Guideline 1.1	Guideline 1.2	Guideline 1.3	Guideline 2.1	Guideline 2.2	Guideline 3
Portugal	Don't know	Don't know	Yes Initiatives such as the POSI programme (Programa Operacional para a Sociedade da Informação)	Don't know	No	
Spain			Yes The Spanish government is investigating the establishment of a working group on the protection of minors from harmful content while using the Internet Action Plan INFO XX		Yes	
Sweden						
UK	No But A survey undertaken by the NOP market research group , revealed that the number of children who would give out their address on the Internet diminished by three quarters between June 2000 and December 2001. This suggests that children absorbing Internet safety messages from multiple sources, know better about the dangers and are changing their behaviour. www.nop.co.uk	No but Five-year study into Internet paedophilia (Cyberspace research unit at the University of Central Lancashire) are calling on schools to take more responsibility for teaching children how to stay safe in cyber-space.	Yes	No	Yes	Yes Home Office screens Internet paedophile warnings ads. The safety messages will be aired at cinemas, on commercial radio stations and in teen magazines in 2002. With £1.5 million of new government funding, the advertisements are designed to educate childre

Country/Actions	National initiatives regarding education of children	Regional initiatives regarding education of children	Cooperation
	Guideline 4.1	Guideline 4.2	Guideline 5
Austria	Yes	Yes	<p>Don't know</p> <p>But</p> <p>To assist lawmakers, the Advisory Council for the Internet and the New Media (www.bka.gv.at/bka/mediem/bin.htm) acts as an informal forum for discussion. Ministries, authorities, industry (ISPA, Chamber of Commerce, etc...), consumers associations (Chamber of Labour, Internet ombudsman, etc...) and NGOs participate.</p>
Belgium	Yes	Yes	<p>Yes</p> <p>Belgium, having three official languages – Dutch, French and German – means that some people report their findings to initiatives or projects in other countries. Nonetheless in Belgium the issue of awareness raising is so important, that it has been set up a network of different partners who co-operate together: ISPA, the Ministry of Justice, the Ministry of telecommunications and the Federal Computer Crime Unit</p>
Denmark			<p>Don't know</p> <p>But</p> <p>Government's inter-ministerial Children's Committee – inter-ministerial working group: Ministry of Justice, the Ministry of Education, the Ministry of Health, the Ministry of Culture and the Ministry of Social Affairs (July 2000)</p>
Finland	Yes	No	No
France	Yes	Yes	Yes

COUNTRY/ACTIONS	National initiatives regarding education of children	Regional initiatives regarding education of children	Cooperation
	Guideline 4.1	Guideline 4.2	Guideline 5
Germany			Yes
Greece	No	No	No
Ireland	Yes		Yes Included in its recommendations was the setting up of an Internet Advisory Board. In October 2001 the IAB launched a number of Internet Safety Initiatives.
Italy	Yes	Yes	Don't know
Luxemburg			
Netherlands	Yes	Yes	Yes In June 1996 Meldpunt (the Dutch Hotline on child pornography on the internet) was officially installed by the minister of Justice. It was the first hotline of this kind in the world and it was run by volunteers, internet aficionados who did not want the internet to be associated with child pornography. In 1998 the ministry justice decided to fund Meldpunt Since 1/1/2000 there is a special police unit on child pornography called 'cyber cops'. Several cases about child pornography have been brought to court and led to prison sentences. This police unit is working closely with the 'Meldpunt Kinderporno op internet', the Dutch Hotline on child pornography on the internet, which has been awarded funding for the years 2000-2003 by the ministry of justice.
Portugal	No	No	No
Spain	Yes	No	No
Sweden	Yes	Yes	No

Country/Actions	National initiatives regarding education of children	Regional initiatives regarding education of children	Cooperation
	Guideline 4.1	Guideline 4.2	Guideline 5
UK	Yes	Yes	<p>Yes</p> <p>The Government has established a Task Force on Child Protection on the Internet, chaired by a Home Office Minister. The Task Force consists of representatives of Children's Charities, the Internet Industry, law enforcement agencies, officials, politicians, civil liberties groups and others. The Task Force helped organise the public awareness campaign described below that can be taken by industry and other matters. There is also a separate strategy group in the Department for Education and Skills, which shares much membership with the taskforce. This is looking at the ways schools access and teaches pupils how to use the internet.</p>

16.

ANNEXES REGARDING AREA OF INTERVENTION D (TECHNOLOGICAL MEASURES)

ANNEX 1

THE INTERNET WORLD¹⁵

1 INTRODUCTION TO THE INTERNET

The Internet is a network that interconnects millions of computers around the world. It is de-centrally organised and any computer can be linked to it.

Physically, the Internet consists of clients, servers and network hardware connecting them.

- *Clients* are the individuals who use personal computers to connect to the Internet.
- *Servers* are computers providing services such as e-mail or file storage for groups of clients.
- The *Hardware* consists of wires, switches, routers, modems, transoceanic cables and satellites.
- *Internet Service Providers* (ISPs) provide access to the Internet. An ISP connects clients and servers to the Internet using telephone lines or other telecommunication channels. ISPs generally also provide their customers with other services such as e-mail accounts, and Web space to publish their own web site, etc...

2 HISTORY OF THE INTERNET

The history of the Internet¹⁶ started with the *ARPANet* network. The *ARPANet* network (Advanced Research Projects Agency Network) was developed for the United States government Department of Defence (DoD) in 1969 in order to provide a secure and survivable communications network for organisations engaged in defence-related research.

This communications network was secure and survivable because the data was distributed in packages. This had two main advantages. This way a big file would not clog up the network and it made the network more secure, since a spy tapping into the network would only be able to intercept pieces of a data transmission. This way of breaking up information is still used for data transportation on the Internet today.

Over the years this network also became accessible to scientific communities. Having used the *ARPANet*, the National Science Foundation (USA) decided to create its own network, and called it *NSFnet*.

From that moment on, other networks started connecting to this backbone, and the growth of the Internet progressed in an exponential way. Even today the Internet keeps on growing by connecting computers all over the world and *NSFnet* still serves as a backbone for the Internet today.

¹⁵ The information contained in this section can be easily found on different Internet sites. However the two main sources for its writing are: <http://www.usus.org/>, and the document "La Lutte Contre la Pédophilie sur Internet: le projet MAPI La Pornographie Infantile sur Internet" <http://www.info.fundp.ac.be/~mapi/mapi-fr.html>.

¹⁶ See also <http://www.pbs.org/internet/timeline/timeline-txt.html>.

3 HOW THE INTERNET WORKS¹⁷

3.1 Protocols

The Internet works on the basis of many different protocols for the exchange of information between different computers. These standards allow computers anywhere in the world to “translate” the digitised information that is located on another computer. Various international organisations such as the World Wide Web Consortium (W3C) are continually negotiating and updating standards for transferring e-mails, documents, images, and so on.

3.2 IP addresses

The different computers that are connected to the Internet communicate with each other by using an addressing system. This system is called IP, which is the abbreviation of Internet Protocol.

Every computer connected to the Internet has a unique address called an IP address. This IP address is composed of a string of numbers that are separated by dots and is provided to a computer by an Internet Access Provider.

Today the “IPv4” IP address system is used. This means that each address consists of 4 series of numbers. Each of the 4 series in an IP address can be a number between 0 and 255. Hence there can be a total of 256 possibilities in each series, and a total of 4.2 billion possible IP addresses (256 x 256 x 256 x 256). An example of an IP address is 209.125.170.30.

Discussions occurring in technical circles have been warning about the fact that we will run out of available IP addresses in less than a decade. Therefore, a new IP address structure is already under work. This new IP address structure is called “IPv6”, which means that this structure is built on 6 series of numbers. This new IP address structure would make it possible to assign a unique reference to every computer in the world.

3.3 Static versus dynamic IP address

Depending on the relationship with the provider, a user can receive a static IP address or a dynamic IP address.

- A *static IP address* means that the user receives the same IP address, each time he connects to the Internet. The provider gives a permanent IP address to the user.
- A *dynamic IP address*, on the contrary, changes each time the user connects to the Internet. The provider assigns an available address to the user when he dials into the provider to connect to the Internet. The user retains that IP address for the duration of the session. When the session is closed, the IP address is assigned to another user.

Each time a computer communicates with another computer, it is the IP address that is used to identify the computers.

¹⁷ Information based on the monthly newsletters of <http://www.htcia.org>.

3.4 Domain Name System (DNS)

Because it is very difficult to remember all these long numbers, the Domain Name System (DNS) system was created. DNS is a global network of servers that translate host names like “www.unisys.com” into numerical IP addresses, like 209.125.170.30. Without DNS, people would have to memorise long numbers instead of intuitive URLs or e-mail addresses.

3.5 How the information travels

The information, or the data, that travels on the Internet is first broken up into a series of packages. These packages are smaller parts of the actual complete data. Each package is then transported separately to the indicated destination. An additional layer (the most commonly used is the Transmission Control Protocol or TCP) ensures that the packages are correctly recombined on the recipient side to form the intended entire message

When a user asks for information from another machine, this request goes first to the user’s Internet provider. The ISP then sends the request to the machine containing the information wanted. On its way to this machine, the request passes through different routers. Routers are devices that pass packets of information from one area of the network to another and choose the best possible route. This is not necessarily the shortest way, but the fastest one, taking into consideration the amount of traffic. For example, the fastest way to travel from Brussels to Paris might well pass through New-York. After the intended machine has intercepted the request, the information requested is sent to the requestor machine. And the message is again broken up into several packages, and passes through several routers.

4 THE WORLD WIDE WEB

4.1 Definition

One of the services offered by the Internet is the World Wide Web. The web is a means of publishing information in order to make it available to the other people who are connected to the Internet.

The information available on the web is published on web servers. Web servers are computers connected to the Internet, which are specifically configured so that the information they store is made available to other computers.

Clients can view the information stored on web servers by using a piece of software called a web browser. Examples of web browsers are *Netscape Navigator* and *Microsoft Internet Explorer*.

By searching the World Wide Web one can find a lot of information. Even though most of the information available on the Web is provided for free, certain pages may only be consulted after paying a fee.

4.2 Web addresses

The documents available on the World Wide Web all have a unique web address, called a “Uniform Resource Locator” (URL). A document URL consists of a protocol name, a domain name, its path and its file name.

- *Protocol*: This is the protocol that will be used to retrieve the document, such as HTTP, for instance.
- *Domain name*: This is the name of the web server on which the document is located. A domain name format is divided into several sections. The number of sections can vary from 2 to about 6. The first section generally contains “www” which stands for the World Wide Web. The last section of a domain name indicates in what type of organisation or in which

country the web server is located. The remainder of the domain name indicates within which organisation, and often in which department, the web server is located. Table 3 shows a few examples of contents of domain names sections and their description.

- *Path*: This is the complete path that has to be travelled in order to locate the document.
- *File name*: This is the name of the document containing the information.

Table 4 – Examples of contents of domain names sections

<i>Type of organizations</i>	<i>Description</i>	<i>Country</i>	<i>Description</i>
.edu	Educational institution	.be	Belgium
.gov	Government	.uk	United kingdom
.com	Commercial business	.fr	France
.org	Non commercial organization	.nl	The Netherlands

On most web servers URLs are case sensitive and the spelling and punctuation must be exactly right in order to be processed correctly.

An example of an URL, together with its structure, is illustrated below:

<http://www.unisys.com/srvcs/networks/default-06.asp>

Protocol Domain name Path File name

4.3 Web pages

The World Wide Web can be used to publish many kinds of files, but the most common are web pages. A web page is a simple text file written in codes according to the HTML standard.

Hyper-Text Markup Language (HTML) is a standard that defines codes for formatting web pages. These codes, also called “tags”, format elements of the page such as paragraphs, fonts, page layout and tables. When accessing a web page, the browser interprets these codes and displays the document in the intended format.

The images that web pages include are not contained in the web page itself. The web page contains codes that indicate how and where the browser has to retrieve these images or other items. Each image is also stored on the web server with a unique URL.

4.4 Web sites

A collection of related web pages and other material is called a web site. The web pages are usually accessible through a home page, which is the first page of the web site.

The user navigates through the different web pages and other material by clicking on links. These links specify the URL of another web page that the browser has to retrieve. The user may also directly type in the URL.

4.5 The process of browsing the Web

Table 5 explains, step-by-step, what happens when a user types in a URL or clicks on a link in a web page to obtain another web page. A simplified architecture of the Web is illustrated in Figure 19.

Figure 19 – Simplified architecture of the Web

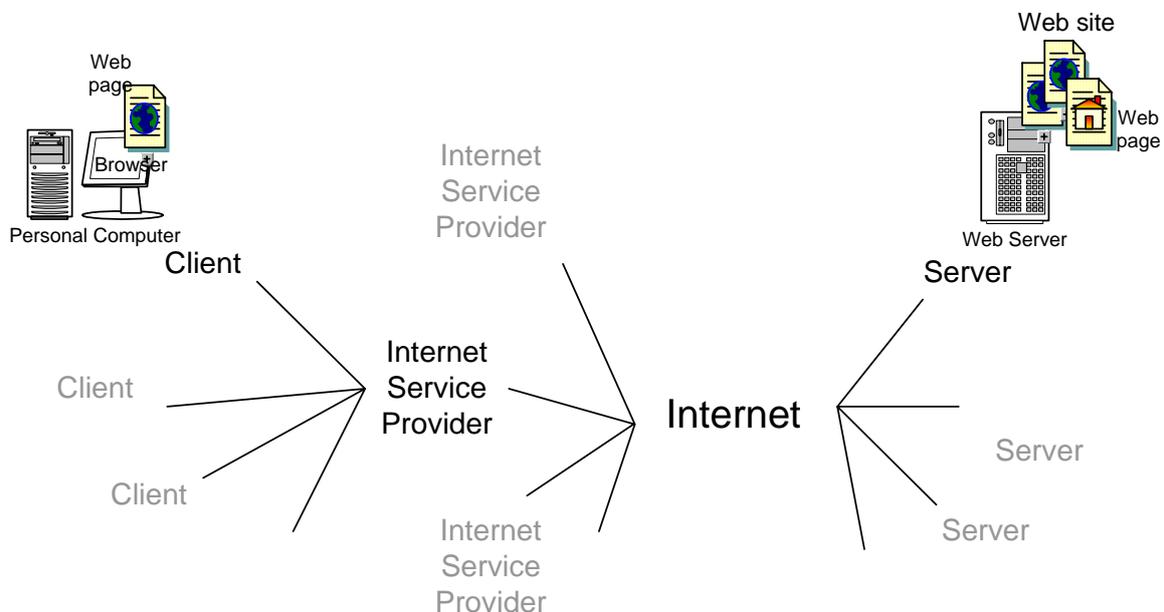


Table 5 - The process of requesting and obtaining a web page

STEPS	USER	CLIENT	INTERNET	SERVER
Step 1	The user clicks on a link or types in a URL.			
Step 2		The browser sends a request for the web page that has this URL.		
Step 3			The request is routed through the Internet to the appropriate web server.	
Step 4				The server retrieves the web page that has the requested URL.
Step 5				The server sends the requested web page back to the client.
Step 6			The web page is passed through the Internet back to the appropriate client.	
Step 7		The browser analyses the web page to see if additional items (such as pictures, for instance) are required.		
Step 8		The browser requests additional items.		
Step 9			The request is passed through the web to the appropriate server.	
Step 10				The server retrieves the requested items.
Step 11				The server sends the requested items back to the client.
Step 12			The items are passed through the Internet to the appropriate client.	
Step 13		The browser assembles all of the received items into a readable document.		
Step 14	The user sees the requested web page.			

4.6 Web applications

Publishing information is one of the functions that web sites provide, but it is not the only one. Other functions exist that are driven by web applications. Web applications are software programs written to allow web servers to respond dynamically to requests they receive. For example buying a book online or searching for a book in an online library database are functions of web sites that need to be responded to dynamically.

5 Electronic mail

Electronic mail or e-mail is a service that uses the Internet network to transport mail and various types of attachments between a sender and an addressee. E-mail resembles paper mail in that it allows people to send a mail from one point to another.

5.1 Format of an e-mail address

Sending and receiving mail requires addresses. The users of the e-mail service need to have an e-mail address and have to know the e-mail address of the addressee.

An e-mail address has the following format: *username@hostname*

- *Username*: This is the "name" of the person. It can be expressed as "first name last name", but this combination is not mandatory. A username can also be a shortened combination of "first name last name" or just an invented name such as "Bart18".
- *Hostname*: This is the name of the mail-server on which a user's mailbox is located. Hostnames are built like domain names and thus also divided into several sections. The number of sections can vary from 2 to about 6. The last part of a hostname indicates in what type of organisation or in which country the mail server is located. The remainder of the hostname indicates within which organisation and often in which department the mail server is located.

An example of an e-mail address, together with its structure, is illustrated below:

sandra.vaesen@be.unisys.com

Username

Hostname

In this e-mail address the username is a combination of first name and last name. The hostname consists of the department Belgium within the company Unisys, which is a commercial company.

5.2 How E-mail works

The e-mail service is offered by e-mail service providers, who host mail servers, whose sole responsibility is to store and forward users' mail messages to the destination mail servers.

To be able to send and receive e-mails the user needs an e-mail client software package. An e-mail client displays a list of incoming messages; has a tool to create new messages and usually provides additional tools. Commonly used clients are *Microsoft Outlook*, *Netscape Communicator* and *Eudora*. Instead of using stand-alone e-mail clients like Outlook, one can also use the services of clients who offer free mail services on their web site. Examples of these clients are *Hotmail*, *AOL*, and *Yahoo*.

E-mail clients have to connect to an e-mail server, which is a machine connected to the Internet running special software to provide people with the e-mail service. The e-mail server is responsible for handling the distribution, forwarding, and receiving of e-mail in a network. Popular e-mail server applications include *Microsoft Exchange*, *Eudora Pro*, *Novell GroupWise* and *Netscape SuiteSpot*.

5.3 E-mail systems

An e-mail system consists of two different servers running on this e-mail server machine: a server for handling outgoing mail – called SMTP server (using the Simple Mail Transfer Protocol) – and another server for handling incoming mail – called a POP3 server (using the Post Office Protocol).

5.4 E-mail headers

A header always accompanies an e-mail message that has been sent. This header contains a lot of information including the identity of the machine used to send the mail.

The following is an example of an e-mail header:

```
From susancwhxtpvn@hud.ac.uk Sun, 21 Apr 2002 06:53:45 -0700
Received: from [204.248.24.189] by hotmail.com (3.2) with ESMTP id
MHotMailBE8C0F31000C400437A4CCF818BDBAF60; Sun, 21 Apr 2002 06:52:49 -0700
To: svaesen@hotmail.com
Date: Sun, 21 Apr 2002 19:55:30 -0500
Message-ID: <1019433330.12656@localhost.localdomain>
X-Mailer: Pine.LNX.4.33
From: susancwhxtpvn@hud.ac.uk
Sender: <susanfityaxkp@hud.ac.uk>
Return-Path: <susanglpxhdyv@hud.ac.uk>
X-Sender: <susantwprswfu@hud.ac.uk>
Reply-To: <susanvovperfk@hud.ac.uk>
Subject: FREE PORN THE BEST ON THE NET!!
```

6 NEWSGROUPS

6.1 Introduction

Newsgroups are virtual places where people who share interests can get together. Newsgroups provide a way to meet and communicate with people from all over the world about these shared interests. Newsgroups provide users the possibility of reading what others are posting (entering) without necessarily responding to it. Anyone can participate in newsgroups, but not all Internet Service Providers offer access to all newsgroups. Today there are thousands of newsgroups on the Internet covering every imaginable topic. These specific topics could be, for example, organic gardening, skydiving, etc. In newsgroups people can also find job postings, business and healthcare advice, announcements about events and even downloadable photos.

To be able to search in newsgroups, the user needs a newsreader program. *Internet Explorer* and *Netscape Navigator* both have a built-in newsreader software. After having chosen which newsgroup the user wants to participate in, he has to subscribe to the newsgroup of interest.

Although most of the information available on Newsgroups is provided for free, some newsgroups can only be consulted after paying a fee.

6.2 Newsgroup names

To facilitate searching the amount of information provided by newsgroups, the information is divided into different groups of topics. The name of the newsgroup indicates the topic of the newsgroup.

Table 6 shows a list of examples of abbreviations that are used in the first part of a newsgroup name to indicate the topic.

Table 6. Examples of Abbreviations of Newsgroup Topics

Abbreviation	Topic
comp	Computers
misc	Miscellaneous
sci	Science
news	News and current events
soc	Social
rec	Recreational
alt	Groups with this abbreviation are groups with alternative subcategories. This second hierarchy was created to facilitate the registering of a new newsgroup, because creating a new group in one of the top categories is more difficult.
...	

6.3 Forums or Discussion Boards

Forums, also called discussion boards, are similar to newsgroups. The difference between forums and newsgroups is that forums exist on a single server that is maintained by its owner. Today, many web sites have their own forums or discussion groups.

6.4 History of Newsgroups

Newsgroups originated in North Carolina in 1979, when two University students started exchanging information with other *UNIX* users. Meanwhile, another student was writing a piece of software that could be used to distribute the information. The work of these three students formed the basis of the newsgroups network, called the *Usenet*.

This network grew and eventually evolved into the newsgroups as they are known today. Nowadays newsgroups are sometimes fee-based, but Usenet continues to reflect its origins as an academic project designed to distribute information freely to anyone who wants it.

6.5 How newsgroups work

Newsgroups are located on special news servers. A newsgroup starts on a single news server and replicates to other servers. Each news server has a special software that maintains a file for each newsgroup hosted by that server. The communication between newsreader and news servers and between news servers is based on

the NNTP protocol (Network News Transfer Protocol). The communication between news servers can also use UUCP (Unix-To-Unix Copy Protocol) for direct connections between *UNIX* servers.

Table 7 explains the working process of newsgroups, from a technical point of view.

Table 7. Newsgroups Working Process

STEPS	DESCRIPTION
1	The newsreader connects to the specified newsgroup. An ISP provides this connection.
2	When the connection is made, the newsreader downloads all the new messages posted in that newsgroup.
3	The user can read the messages and reply to them.
4	The user may also choose to start a new thread. A thread is a post and the series of messages replying to it.
5	If the user wants to start a new thread then the newsreader sends the messages to the news server.
6	The news server saves the messages in the file for that newsgroup. A newsgroup file is a large text file where each new message is appended. After a certain length or time, the messages at the beginning of the file are removed and placed in a newsgroup–archive text file.
7	The news server connects to one or more other news servers and sends the updated information. Each news server compares its own file for that newsgroup with the files it receives for that same newsgroup. It adds any difference that it finds. The news server then sends the combined information to other news groups.
8	The newsgroup changes are replicated to each news server until all of them have updated the information. This process is ongoing.
9	Other subscribers can read the messages sent by the user and reply to them.
10	The user can again see their replies and the newsgroup process repeats itself.

6.6 Subscribing to a Newsgroup

The first thing the user needs to know to subscribe to a newsgroup is the name or the IP address of his ISP's news server. If the user's ISP does not have any news server, as is the case sometimes, the user can refer to a publicly accessible news server.

A newsreader program is necessary in order to be able to subscribe to a newsgroup. This can be a special software such as *Microsoft Outlook Express*, which contains a newsgroup tool. *Internet Explorer* and *Netscape Navigator* both have a built-in newsreader software. Both types are client software.

A newsreader client software allows newsreader information (Name or IP address) to be configured. For example, *MS Outlook Express* uses a wizard to guide users through the process of adding a news server. When a news server is added, a list of newsgroups provided by this news server is shown. A news server does not carry every newsgroup available, but the user can request to add a newsgroup.

In the list of newsgroups one then has to select the newsgroups he is interested in and click the “Subscribe” button. Then one can visualise the messages related to a newsgroup by clicking on the name of that newsgroup.

6.7 Creating a newsgroup

Creating a newsgroup is a process that takes time and requires patience.

The first thing the originator of a newsgroup has to do to create a newsgroup, is to post a Request for Discussion (RFD) to the newsgroup “news.announce.newgroup”. This RFD has to describe the purpose of the newsgroup and include the proposed name. It must also specify a list of the categories of topics that the newsgroup will cover.

Newsgroup readers then read the RFD and make comments and suggestions. This discussion can last for about a month or even longer when it is carried out by mail.

When the discussion is completed, the originator has to request a Call for Votes (CFV). He does it, again, by posting a message to “news.announce.newgroup”. The CFV duration is 20 to 30 days during which newsgroup readers may vote. Once the vote is over, the votes are counted and the results are posted in “news.announce.newgroup”. This takes another mandatory five-day period during which counting and corrections take place.

Then the decision is taken whether to create a new newsgroup or not. Three criteria must be met for starting a newsgroup:

- At least two-thirds of the votes must be in favour of the newsgroup.
- The number of votes in favour of the newsgroup must be at least 100 more than the votes against it.
- There must not be serious and demonstrable objections to the creation of the newsgroup.

Once the newsgroup is accepted, it is created and announced in “news.announce.newgroup”. From that moment the newsgroup is ready to accept posted messages.

7 Internet Relay Chat (IRC)

The chat service¹⁸ offers a way to communicate synchronously across the Internet. It offers the facility of instant and real-time access to people of all ages and backgrounds from all around the world. It enables children and adults alike to interact on the same “playground”, regardless of the many social, cultural, religious, geographical or potentially discriminatory obstacles that usually inhibit them offline.

The most common versions of chat are Internet Relay Chats (IRC) and Web-based chats. An IRC consists of multiple servers connected to each other, whether web-based chats run either on dedicated web sites or on individual homepages running a chat facility.

IRC is not under the control of any organisation and uses open standard software, enabling anyone with sufficient knowledge to write and operate an IRC program.

People meet each other in virtual rooms and communicate there with each other using nicknames to identify themselves without revealing their real identity. One may only communicate with people who are connected to the Internet at that moment and thus online. Communication usually takes place via written text.

¹⁸ The information in this section is mainly based on the site: <http://www.newircusers.com/network.html>.

7.1 How IRC works

To use IRC, the first requirement is to have an IRC program, also called an IRC client. A wide variety of IRC programs are available on the Internet. An example of a Windows based IRC client is *mIRC*.

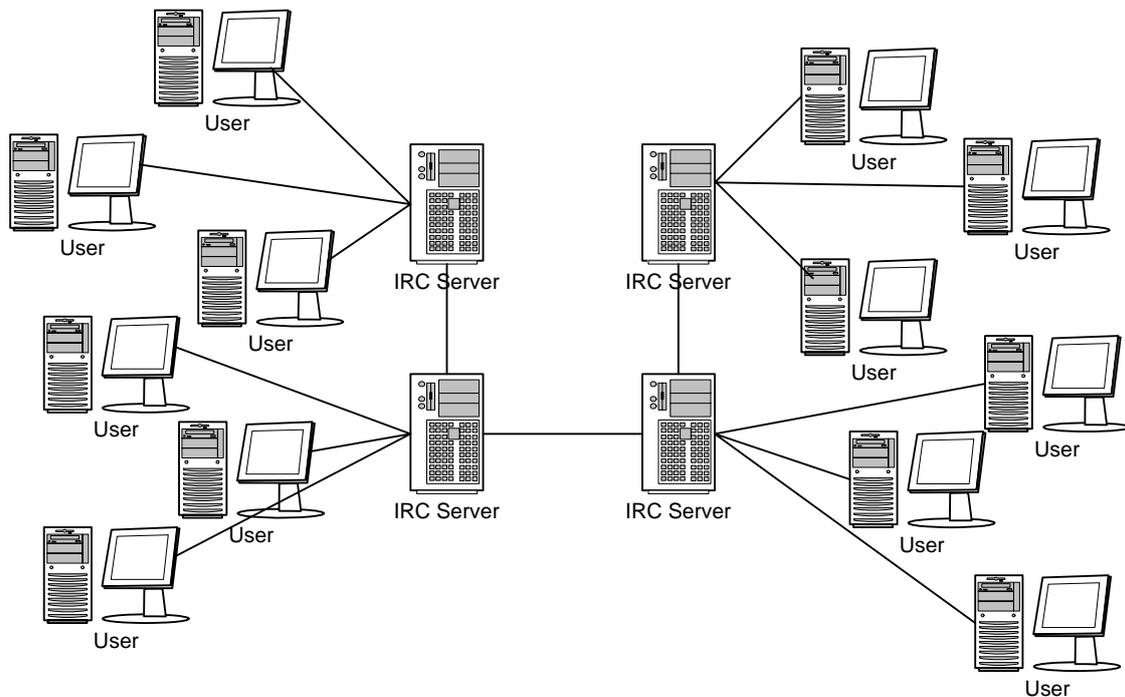
IRC is also based on the client-server model, or Network. To use the IRC service on the Internet, the user's machine has to connect to an IRC server in an IRC network. An IRC network is a collection of IRC servers linked together (see Figure 20 for an illustration). When logging on to the IRC network, the IRC client connects to one of the IRC servers on that network.

All IRC servers in the network share and have access to the same information. Each server knows who is on the network, which chat rooms the users are in, and which servers the users are using.

IRC Networks vary in size. Smaller ones may consist of only 2 servers and have less than 100 users. Others can have over 100 servers and more than 20,000 users!

There are many IRC networks. Each network is a separate entity on its own. One network does not connect to another network. The networks do not share common servers. An IRC user cannot talk to a user that is not on the same network as himself.

Figure 20 - An IRC Network



7.2 IRC Network services

IRC networks provide a range of network services to their users. Networks usually run two basic services, *Chanserv* and *Nickserv*. A third service, called *Memoserv* can also be run in conjunction with *Nickserv*. These services are run in the IRC networks as stand-alone servers and they usually work in the background of the network. The services can vary in form, implementation and complexity from network to network, but their function is always the same:

- *Chanserv* allows users to register a channel (chat room) on an IRC. A registered channel is protected so that no one can take-over the channel. The channel owner, that is to say, the person who registered the channel with *Chanserv*, can specify who gets operating privileges by composing a list of operators. The owner can set the channel topic, modes, and ban lists.

All these functionalities are maintained and enforced by *Chanserv*, unless the channel owner changes them.

On most networks the registration of a channel expires if the channel is not used for a certain period of time, ranging from 14 to 30 days.

- *Nickserv* allows users to register their IRC nickname (or “nick”), a sort of alias. Once a nickname is registered, no one else can use this nick. The nick is identified by the logon address and is password protected. Each time a user wants to register a nickname, the *Nickserv* service checks if the nickname used matches the logon address of the user. If they do not match, the service warns the user to choose another nickname or else he will be kicked out of the IRC network by the service.

On most networks the registration of a nickname expires if the nick is not used for a certain period of time, ranging from 14 to 30 days.

- *Memoserv*, which is run in conjunction with *Nickserv*, allows users with a registered nick to send and receive memos to and from other users with registered nicknames. This is a sort of IRC e-mail.

8 File Transfer using File Transfer Protocol (FTP)

Transferring files using the Internet is another commonly used service. Files are transferred across the Internet using the File Transfer Protocol (FTP). FTP is also used to update (delete, rename, move and copy) files on a server. The File Transfer protocol is one of the suites of protocols that are part of TCP/IP.

FTP is particularly useful for the exchange of large files between computers. Files made available through FTP can be in any format, such as document files, multimedia files, or application files.

FTP can be used to transfer files within a company, for instance, from one computer to another computer. The remote computer can be of any kind, it does not need to have the same operating system. It can also be a server. FTP can also be used to download an updated version of a browser for instance.

Another frequent use of FTP is the uploading of Web pages to the World Wide Web. This is how all Internet files are changed or updated.

To use FTP, an FTP client is needed. This software is available from most Internet providers, and many operating systems have an FTP interface. Moreover, when Web browsers allow users to download files from the Internet, they use FTP without prompting the user to start another program. FTP client can also be downloaded from the Internet, for example, *WS_FTP*, *LeechFTP* and *CUTE_FTP*.

To be able to transfer via FTP, the target site must have an active FTP server or service.

8.1 FTP via a Web Browser

To access an FTP server using a web browser the FTP URL has to be used: *FTP://<server>*. In this URL format <server> has to be replaced by the name of the server.

When the user's machine is connected to the FTP server, the user can see in his browser window all the directories and files that are located on the FTP server. To download a file, the user selects the desired file or directory and a "Save as" window appears. Then the user selects the location where he wants the file or directory to be stored on his machine.

The browser can also be used to upload files. This can only be done when the FTP server used and the selected directory are configured for "write" operations. To upload files, the user first selects the FTP server using the FTP URL. Then he chooses the upload or publish function of the web browser. A file upload window appears and finally, the user selects which file to upload.

8.2 FTP via a Standalone Client

Once the FTP client is installed, a connection with the server has to be established. To open an FTP session, three pieces of information have to be provided to the client:

- The name of the server to which the user wants to connect;
- A user name;
- A password.

Once the user is logged in, the client will show a list of directories (folders) and files. After selecting the files the user wants to download (or upload), the client will start transferring the files.

ANNEX 2

APPENDIX 1: PRODUCTS SPECIFICATIONS SHEETS

A.1. ACCESS MANAGEMENT ENGINE OF BASCOM	365
A.2. ACTIVITY MONITOR OF TRUEACTIVE SOFTWARE	369
A.3. AOL PARENTAL CONTROLS OF AOL.....	374
A.4. BOUNCE OF ONE LIGHT CORPORATION	378
A.5. BROWSERLOCK OF DRAGON ENTERPRISES	382
A.6. BSECURE OF BSAFE ONLINE.....	386
A.7. CHIBROW OF PEOPLENET INTERNATIONAL	390
A.8. CHILDSAFE OF WEBROOT SOFTWARE	394
A.9. CLEANWEB FILTERING SERVICES OF 711.NET.....	398
A.10. COMPUTER COP DELUXE.....	402
A.11. CONTENTKEEPER WEB FILTERING	406
A.12. CONTEXION OF RULESPACE INC.	410
A.13. CYBER SENTINEL OF FINER TECHNOLOGIES INC.....	414
A.14. CYBER SNOOP OF PEARL SOFTWARE INC.	418
A.15. CYBERPATROL OF SURFCONTROL INC.....	422
A.16. CYBERSITTER OF SOLID OAK SOFTWARE INC.	427
A.17. dSPAM OF DRAGON ENTERPRISES	431
A.18. ENUFF OF AKRONTECH	435
A.19. eTRUST INTRUSION DETECTION OF COMPUTER ASSOCIATES.....	440
A.20. FILTERPAK OF S4F.....	444
A.21. FIRETRUST MAILWASHER	448
A.22. FREEDOM PARENTAL CONTROL OF ZEROKNOWLEDGE.....	453
A.23. IF-2003 OF TURNER AND SONS PRODUCTION INC.	457
A.24. I-GEAR OF SYMANTEC CORPORATION	461
A.25. INTERNET SHERIFF OF TEL.NET MEDIA	466
A.26. iWAYPATROL OF ITECH INC.....	471
A.27. KIDSAFE EXPLORER OF ARLINGTON SOFTWARE.....	476
A.28. KIDSNET	480
A.29. KIDWEB.....	484
A.30. KIDZ.NET OF KIDZ.NET NATIONAL PTY. LTD.	488
A.31. LINE-LOC.....	492
A.32. MAILWASHER	496
A.33. MARANATHA FILTER.....	500
A.34. MoM OF A. VALUE SYSTEMS	504
A.35. N2H2 OF SECURE COMPUTING	508
A.36. NET GUARDIAN OF MAXIMUM INTERNET LIMITED.....	512
A.37. NETFILTER OF NXP TECHNOLOGIES	516
A.38. NETIQ WEBMARSHAL OF ANCORIS LIMITED	521
A.39. NETNANNY OF BIONET SYSTEMS	526
A.40. NETPROTECTOR OF THE MODEM LOCK COMPANY	530
A.41. NORTON INTERNET SECURITY OF SYMANTEC CORPORATION	534
A.42. OPTENET.....	539
A.43. PERKEO++ OF AUTEM GMBH	543

A.44. PURESIGHT OF ICOGNITO	547
A.45. R3000 OF 8E6 TECHNOLOGIES	551
A.46. SENTRYCAM.....	555
A.47. SMARTFILTER OF SECURE COMPUTING	559
A.48. THE SPAMCOP EMAIL SYSTEM OF SPAMCOP.....	564
A.49. SURFCONTROL TOTAL FILTERING SOLUTION	568
A.50. THE BAIR OF XEXOTROPE.....	573
A.51. TOO COOL OF SOFTWARE 2010.....	577
A.52. WATCHDOG.....	581
A.53. WEBDOUBLER OF MAXUM DEVELOPMENT CORP.....	585
A.54. WE-BLOCKER	589
A.55. WESENCE	593
A.56. WISECHOICE INTERNET FILTERING	597

A.1. Access Management Engine of BASCOM

Unisys

NAME and version of the product:

Access Management Engine (AME)

Company (name and address):

BASCOM

275 Marcus Blvd, Suite R

Hauppauge, New York 11788

Voice: 631.434.6600

Fax: 631.434.7800

URL Home site:

<http://www.bascom.com/solutions/ame.shtml>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
- Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

The specific protocols that are controlled aren't really specified on the website. They speak about Internet in general.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list**
 - White list**
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not specified on the website.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not specified on the website.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate – Business

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not specified on the website.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
A customer administrator can modify and save zone configurations via Lesson Profiles to be applied to different computers, as necessary. If the host requires the zones to be set up differently, then BASCOM will work with them.
For instance, to meet the need of schools, a fourth zone was offered with a pre-determined list of educationally focussed Web sites presented through a portal.
- Security
Since AME for ISPs resides at the Host's network centre, it is far less likely to be tampered with or circumvented.
- Technical Requirements (Platform, type of browsers compliant with,...)
No client-side software is required and it works with any form of Internet access delivery, e.g. dial-up, ADSL, cable, etc.
- Configuration
Bascom provides the user with an Easy-to-use, Web-based administration. And immediate turn-on/turn-off capability of filtering is available.
- Support
Special web forms for support and FAQ pages are available.
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
Not specified on the website.
- Extra, useful information about the product / Documentation
/

A.2. Activity Monitor of TrueActive Software

NAME and version of the product:

Activity Monitor V5

Company (name and address):

TrueActive Software

401 Parkplace, Suite 100

Kirkland WA 98033

USA

URL Home site:

<http://www.TrueActive.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
- Conventional proxy application
- Transparent proxy application
- Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
It is a complete Activity Monitoring tool.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

The product monitors and reports on all activities, providing an audit trail and a "deterrent" rather than preventing access. For example, all websites that have been accessed are recorded, optionally with screen shots taken. This can then be investigated later on.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

The approach is deterrent rather than control. Filtering & blocking applications often have loopholes. TrueActive monitoring deters users from certain activities.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Not applicable – see question 4

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

Not applicable – see question 4

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Law enforcement, prison services, investigative government agencies

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
The person responsible for the monitoring of the system will be alerted via email. The approach is deterrence, not prevention.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
TrueActive even records both sides of a chat room, email or instant messenger conversation. For example, if a child is online talking to an adult, the full conversation will be recorded and stored in a database protected by a 128-bit MD5 digital signature to prevent tampering. This level of database protection means that the recording can be used in a court of law.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: All activity is recorded for review. Certain keywords can promot an immediate review.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not applicable – see question 4

14. Product description:

- Options
TrueActive's foundation suite contains the software needed to monitor all the activity on one PC and to report on that activity.
In addition, TrueActive has several optional features, for example:
 - network manager, allows you to control a network of monitored PC's from a central location.
 - data management for large systems, this allows for automatic archival and deletion of unwanted data.
 - stealth email, for collecting data from remote PC's being covertly monitored
 - key phrase alert via email, allows immediate alerts to be sent to a supervisor when a keyword is typed in or appears in a Windows caption.
- Security
TrueActive can run overtly or covertly. All data is protected with a 128-bit MD5 signature, which means that data can be used as evidence in a court of law. Product configuration options and the setup program are password protected to prevent any unauthorised changes.
- Technical Requirements (Platform, type of browsers compliant with,...)
TrueActive runs on all Windows platforms from Windows 95 to XP. Once installed it will record all browsers, email systems, messenger applications, every windows application – this is a key strength over many filtering & blocking applications. There are no loopholes.
- Configuration
TrueActive is installed through a simple wizard and runs as a Windows service. If running on a network, a standard configuration can be setup and/or modified and distributed to all users.
- Support
The company provides support via email, included in the standard annual subscription. Optionally, they can provide telephone support for an upgraded subscription.
On-site consultancy can be provided across Europe on a time and materials basis.
- Updates
Updates and new version are provided elctronically. If installed on a network, the latest version can be automatically downloaded and distributed to all PC's.
Updates are included as part of the annual subscription.
- Prices (product, support, updates,..)
The price varies depending on the number of licenses required, features required etc. The product is licensed on an annual subscription basis, which includes program updates and email support.
- Extra, useful information about the product / Documentation

TrueActive is being used by over 7000 customers in over 70 countries, including families, governments, public bodies and commercial organisations.

The approach to being safe online is very different. Instead of blocking or filtering material (which is an almost impossible race as thousands of new sites, pages and images come online every day) they give the user some responsibility to use the web, email and other applications in an appropriate way. With blocking & filtering, users can often look for security loopholes, or new techniques to evade system control. If the person knows that they are being monitored , it does not matter what techniques are tried, all online activity will be seen and recorded.

TrueActive believe that only through behaviour modification real and permanent change will occur.

A.3. AOL Parental Controls of AOL

Unisys

NAME and version of the product:

AOL's Parental Controls

Company (name and address):

AOL

URL Home site:

<http://www.aol.com/info/parentcontrol.html>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list**
 - White list**
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

AOL parental controls also allow to limit how long other screen names can be logged on for, even during specific time periods.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

AOL uses the control lists provided by "The Learning Company", which also produces its own filtering product, Cyber Patrol.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

Violence, gambling, etc.

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options

If you do find that a total stranger has managed to get into the same circle of online friends as your child, their screen name can be added to the list of blocked screen names under Settings,

Preferences, Privacy. Additionally, contact the parents of your child's other friends and encourage them to do the same. If the stranger resurfaces or will not go away, one can notify AOL member services right away. Any threats report to your local police.

- Security
The different accounts (administration and other users' accounts are password protected.
- Technical Requirements (Platform, type of browsers compliant with,...)
Users have to register for an AOL ISP Connection.
Users do not need to install any extra software to use the filtering services of AOL.
- Configuration
Can be done via their website, on the pages you get access to via registration.
- Support
In the countries where AOL is based, local support is available 24 hours a day, seven days a week by calling a special number. One can also email the questions to a special email address.
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
AOL is an ISP and the control service is provided to their member as built-in front-end feature of their subscription.
- Extra, useful information about the product / Documentation
<http://surfsafely.com/surfsafety/news/2003-01-05.html>

A.4. Bounce of One Light Corporation

NAME and version of the product:

Bounce 2.0

Company (name and address):

One Light Corporation

734 W. Whitney Ct. Eagle ID

USA 83616

URL Home site:

<http://bouncefilterware.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
- Conventional proxy application
- Transparent proxy application
- Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
 - Server or ISP
 - ISP and User
-

4. Which type(s) of technology does the product implement for control?
- Site labels or rating systems (PICS, an independent rating system)
 - List of URLs
 - Black list
 - White list
 - List of keywords
 - List of keywords combined with analysis of the context in which they appear
 - Analysis of image content
 - Packet analysis
 - Authorization
 - Activity tracing
 - Other, please specify:
5. By whom is the classification of the content done?
- Content providers
 - Third-party experts
 - Local administrators
 - Survey or vote
 - Automated tools
 - Other, please specify:
6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,
- (a) N u d l t y (partial or full)
 - (b) A d u l t p o r n o g r @ p h y
 - (c) C h i l d p o r n o g r @ p h y
 - (d) A n i m a l p o r n o g r @ p h y
 - (e) G r o s s d e p i c t i o n s
 - (f) S e x e d u c a t i o n
 - (g) O t h e r , p l e a s e s p e c i f y :
gambling, violence, racism
7. Which type(s) of public (“buyers”) is targeted?
- Parents
 - Schools
 - ISP
 - Public points of access such as libraries,...
 - Other, please specify:
8. Can the product be used without the knowledge of the person (child) being controlled?
- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
A dialog appears to add the site to the White List if the administrator sees fit, or if the site was unnecessarily blocked by the filter.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

According to Bounce, they have never had a complaint.

The following page gives a good idea: <http://bouncefilterware.com/reviews.php>

14. Product description:

- Options
Realtime filtering, Activity Log, Time control, Restricted & Permitted site lists, Bounce System Monitor, Multiple-User design, User Wizard.
- Security
Passwords are not "crackable"; hashes of passwords are stored in Windows registry. Administrator controls are password-protected. System Monitor application accompanies main browser application to prevent children from executing programs chosen by the administrator. Internet Explorer and Netscape are restricted programs by default.
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 98 to XP, Internet Explorer 5.0 required
- Configuration
Parents can create, modify, and delete your children's accounts with a wizard.
- Support
Installed documentation in product.
Support can also be asked on the web site by submitting a web form.
- Updates
Available free of charge from website.
- Prices (product, support, updates,...)
Bounce is a free web browser.
- Extra, useful information about the product / Documentation
As Bounce is a free web browser, donations are appreciated @
<http://bouncefilterware.com/donate.php>

A.5. BrowserLock of Dragon Enterprises

Unisys

NAME and version of the product:

BrowserLock v7.37

Company (name and address):

Dragon Enterprises

69 St Mildreds Road

Westgate on Sea

Kent CT8 8RL, UK

URL Home site:

<http://www.browserlock.co.uk>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
The users.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable (white list approach).

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

100%

14. Product description:

- Options
Home, Business and Kiosk Editions are available.
- Security
Password-protected access to setup, anti-tampering measures.
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 32-bit, compliant with Internet Explorer, Netscape
- Configuration
/
- Support
Available by email and fax.
- Updates
Uses a user-defined white list.
- Prices (product, support, updates,..)
Starting from £34.99.
- Extra, useful information about the product / Documentation
Free 30 day trials available

A.6. Bsecure of Bsafe Online

NAME and version of the product:
BSecure version 4.1
Company (name and address):
Bsafe Online, Inc.
99 Eglin Parkway Suite 1D
Fort Walton Beach, Florida, U.S.A. 32548
+01 662.422.1984 Mobile contact
URL Home site:
<http://bsafeonline.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Thin Client-Server Web-Services based web and application filter.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Includes Firewall, Intrusion detection, spyware/adware filter, P2P and pop-up killer which often are sources for child and/or other pornogr@phy. Spam filter add-on due in Dec 31, 2003.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Application control, server based history reporting.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
They employ 8e6 Technologies database as well as their own Bsafe patent pending "Deep Web" technology that finds hidden and unlisted/unlinked sites.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Currently 36 categories, December 2003 will have 76 categories based on 8e6 Technologies' list. Animal porn would fall under general porn. Also categories like R-Rated, Explicit Art, Obscene, etc. (They produce the 8e6home.com private label also.)

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Churches

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Categorized history reporting emailed to single or multiple addresses.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

History reporting is tamper proof because it is at the server level and not in a file on the personal computer. Currently it captures summary and detail data on web sites visited, compares blocked vs unblocked, time usage, multiple user reporting, etc. Currently adding IM, ftp, P2P, games and other application usage tracking history.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: User can review & modify application and port lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

98%

14. Product description:

- Options
Filter, Firewall, Intrusion Detection, Pop-up and spyware killers are standard
Reporting, Virus and Spam features are optional
- Security
Thin Client encryption of all authentication and billing info. Fully redundant provisioning and filtering network on OC48 superhub with backup locations.
- Technical Requirements (Platform, type of browsers compliant with,...)
All Windows (except 3.1) Mac OSX (Jan '04) All browsers, Anywhere in the world. 1MB application requires very little system overhead.
- Configuration
Ability to set multiple custom user profiles. Profiles created automatically for 2000, NT and XP platforms. Settings are set to default, with the user not needing to make complicated installation decisions. Can go back and change at any time.
- Support
Over 800 Knowledge base entries, 24 hour email support, 7:00-9:00 CST phone support. Also setting up Dublin, Ireland filter and support center in early 2004.
- Updates
Automatic updates are realtime and server based, so the client does not need to be updated. Profile updates are made from any browser and can be made in group, subgroup or individual levels. Changes are automatically updated at authentication. Product software upgrades can be ad hoc or pushed to the client. Adding a new service like reporting is a simple profile change that does not require a software upgrade. Simply re-authenticate and the function is active.
- Prices (product, support, updates,..)
49.95 USD Filter, Firewall, ID, Pop-up killer and Spyware killer
59.90 USD Above plus Reporting.
69.90 USD Above plus Anti-Virus for All-in-One suite.
Spam filter add-on (Jan '04) not priced.
Quantity discounts reduce price significantly. We are also creating a private label Safe@Omada to be sold through Dublin to Europe that will be in Euro and local currencies.
- Extra, useful information about the product / Documentation
Bsafe Online has dedicated itself to protecting families of the world from dangers on the Internet. Most filtering companies have their primary business and main source of revenue in the Enterprise to protect against lawsuits and lost productivity. Bsafe has dedicated itself and invested millions in the more difficult job of protecting children against the many sources of danger.

A.7. ChiBrow of PeopleNet International

Unisys

NAME and version of the product:
CHIBROW 7.0 – The Childrens Browser
Company (name and address):
PeopleNet International, Corp.
1600 Adams Dr.Menlo Park, CA 94025
URL Home site:
<http://www.chibrow.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Monitor internet usage and other application on the computer.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
violence, hate speeches and profanity

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
ChiBrow ignores the blocked URLs and sends an alert at the bottom of the browserscreen.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Parents customize settings for each user, including default homepage, Safe-Sites List, search engine, time, and more.
 - Parents can decide whether their child can only visit the exact site name, or other sites that may belong to the same domain.
 - Parents can use their Safe-Site List elsewhere; they can even create different Safe-Site lists for different children.
 - Parents can set a weekly schedule for when your child can use the Internet. Parents can disable safety to go to any site (by typing in the Web address).
 - Parents can regulate access to all sites belonging to schools (.edu), government (.gov), and organizations (.org); by default and for security reason, access to .org domains is disabled.
- Security
 - The administration facilities are password protected.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Pentium 133MHz or Faster IBM PC compatible
 - 32MB of RAM (64MB recommended)
 - 30MB of free hard disk space
 - Microsoft Window 95, 98, NT, 2000, ME or XP
 - CD-ROM drive required for software installation
 - Microsoft Internet Explorer 5.x or higher
 - Internet Connection

ChiBrow isn't available for macintosh.
- Configuration
 - A special Administration Panel for Parents is available.
- Support
 - A complete help/user guide is included in ChiBrow self by clicking on the "Help" or question mark icon of ChiBrow.
 - Online web and email support is provided as well.
- Updates
 - Not specified on the website.
- Prices (product, support, updates,..)
 - \$ 29.99 USD per License
- Extra, useful information about the product / Documentation/

A.8. ChildSafe of Webroot Software

Unisys

NAME and version of the product:

ChildSafe 3.0

Company (name and address):

Webroot Software

Unit 14, Distribution Centre,

Shannon Ind. Estate,

Shannon, Co. Clare,

Ireland

URL Home site:

<http://www.webroot.com/wb/products/childsafe/index.php>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Monitoring and web blocking software

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Violence, Hatery, Gambling, Dating, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Key stroke capturing

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
Stealth or visible monitoring
Run Child Safe in the background, completely hidden or in plain view, to watch as much or as little of your children's computer and Internet activity as you choose.
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 95, 98, 2000, ME or NT4
90 Mhz processor
5 MB hard drive space
8 MB RAM
- Configuration
An easy-to-use interface puts you in control of which activities to monitor, when the program is run, and how many logs the program will create.
- Support
Free for customers
Online/Phone/Email support
- Updates
All customers who purchased software from Webroot Software are eligible for free software updates within one year of their original date of purchase (or the purchase of a registration renewal).
- Prices (product, support, updates,...)
\$29.95
- Extra, useful information about the product / Documentation
/

A.9. CleanWeb Filtering Services of 711.Net

Unisys

NAME and version of the product:

CleanWeb Filtering Services

Company (name and address):

711.NET Inc

2063 N Lecanto HWAY

Lecanto

FL 34461

URL Home site:

<http://www.cleanweb.net/>

1. Product type:

Special purpose browser for children

Special search engine and portals

ISP application

Conventional proxy application

Transparent proxy application

Specialized cache engine

Restricted access application (e.g. by using age verification)

Personal Computer application (Filter)

Other, please specify:

People not able or not prepared to use the ISP service can always order a CD-rom version of their filter.

2. What does the product control (the scope)?

Access to web pages

Use of e-mail

Spam

Attachments of emails

Online chat rooms

Movement of files in and out of your computer (FTP)

Access to newsgroups (Usenet)

Access to various forms of instant messaging

E-commerce, credit card usage

Offline (non-Internet) computer use

Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: People can inform the company about inappropriate web sites via an online form.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on their website.

14. Product description:

- Options
Both Filtered Internet Access and a Filter Only service are available.
- Security
Not specified on their website.
- Technical Requirements (Platform, type of browsers compliant with,...)
No special requirements are mentioned.
- Configuration
Not specified on their website.
- Support
Technical and Customer Service Staff at any time, 24/7 using phone and email.
- Updates
Not specified on their website.
- Prices (product, support, updates,..)
Filter Only Monthly \$4.95 / month No Pre-Payment
Filter Only Annual \$4.08 / month \$49.00 Pre-Payment
- Extra, useful information about the product / Documentation
This is a service, only applicable for customers in USA.

A.10. Computer Cop Deluxe

Unisys

NAME and version of the product:

Computer Cop Deluxe

Company (name and address):

ComputerCOP

1 Corporate Drive, Suite 103

Bohemia, NY 11716 , USA

URL Home site:

<http://www.computercop.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

A dictionary of keywords and phrases including Emoticons (kid's secret online language) is used.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
A keystroke-monitoring tool.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Not specified on the website.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
ComputerCOP's law enforcement products are used by the U.S. Army, the F.B.I., U.S. Probation and sheriff departments, police departments, county and state probation departments and district attorneys and transit authority offices throughout the country
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
The tool is compatible with Windows 95,98,Me, NT, 2000, XP.
For Mac :
 - o PowerPC® processor
 - o Mac OS software version 8.5 or higher
 - o 16 MB of available RAM (24 recommended)
 - o 2 MB of available hard-disk space
- Configuration
ComputerCOP's products are developed on the philosophy that sophisticated technology can and should reside in an easy-to-use interface.
- Support
ComputerCOP offers free technical support to all registered and/or certified users from Monday to Friday 8:30 am to 5:30 pm EST.
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
\$39.95
- Extra, useful information about the product / Documentation
ComputerCOP software scans a computer and provides owners a simple method to see if the computer has been used inappropriately.

A.11. ContentKeeper Web Filtering

NAME and version of the product:

ContentKeeper Web Filtering

Company (name and address):

ContentKeeper Technologies

URL Home site:

<http://www.contentkeeper.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Web Filtering Appliance and/or Web Filtering Software-only solution.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Controls file downloads e.g. MP3, Video, Games and blocks web based virus attacks
NOTE: Anti-SPAM and Anti-virus modules for SMTP mail will be added to ContentKeeper in March 2004.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

ContentKeeper Live Blocking analyses the URL, Metatags, Words and phrases on the page, web page geometry and hyperlinks in order to correctly categorise web pages and add them to the ContentKeeper filtering database.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

The global community of Network Managers and Authorised teaching staff using ContentKeeper may add or modify the classification of any web-page. ContentKeeper research staff will check the addition or re-classification request before modifying the Global database.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

The above are all sections of the Adult Content category except S e x e d u c a t i o n which falls into the Education category and so can be filtered separately.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

Companies specialising in providing Internet solutions to the Education sector. Local Education Authorities. Grids for Learning. Internet cafes. Learning Cafes.

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

Realtime reports and off-line reports using WebSpy Report Generating tool

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Estimated at 98.7%

14. Product description:

- Options
ContentKeeper can be supplied as a Purpose-built Filtering Appliance or as a Software only solution that can be installed on a standard Intel based server or PC.
- Security
All software and databases are encrypted. All communications with ContentKeeper filters is encrypted. There are no open ports available on the filtering device. Client confidentiality is assured.
- Technical Requirements (Platform, type of browsers compliant with,...)
Either ContentKeeper LE Appliance
Or 1.2 GHz (or higher) Intel based Server, 512 Mbytes RAM, 20 GByte Hard Disk, 3 Intel Pro/100 Ethernet NIC.
ContentKeeper can be used virtually any network without re-configuring existing network devices such as firewalls and proxy servers. Compatible with all Internet Browsers and network operating systems.
- Configuration
GUI accessed through a standard Web Browser e.g. Internet Explorer
- Support
First level provided by worldwide Resellers and Distributors.
Second Level provided by ContentKeeper Technologies offices around the world.
- Updates
Regular updates are provided on-line and at no cost.
- Prices (product, support, updates,...)
Price is for a software license based on the number of PCs on the network requiring filtering. Special reduced prices are offered to Educational customers and for Education Authorities providing filtering for a large number of schools.
Price example: For a school with 250 PCs, the price of a 1 year software license is 2188 Euros, which includes, support and updates.
Cost of server hardware is additional to the above price. Purchase guide price for the ContentKeeper LE Filtering Appliance is 1275 Euros.
- Extra, useful information about the product / Documentation
ContentKeeper software can be downloaded from our website and evaluated for 20 days without charge. A full Administration Manual is provided with the product as well as Release Notes describing the newest features recently added to the product.
ContentKeeper Technologies has appointed resellers and distributors in most countries. These partners will provide local installation, training and on-going support to ContentKeeper customers.

A.12. Contexion of RuleSpace Inc.

NAME and version of the product:

Contexion

Company (name and address):

RuleSpace, Inc.

111 SW 5th Ave

Suite 2100

Portland, Oregon

97204

URL Home site:

www.rulespace.com

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

- YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

99.94 %

14. Product description:

- Options
ASP based or locally hosted.
- Security
/
- Technical Requirements (Platform, type of browsers compliant with,...)
All browsers are supported.
- Configuration
Basic and advanced configuration is provided.
- Support
Full technical support is provided.
- Updates
Updates are daily handled.
- Prices (product, support, updates,..)
/
- Extra, useful information about the product / Documentation
/

A.13. Cyber Sentinel of Finer Technologies Inc.

NAME and version of the product:

Cyber Sentinel 2.0

Company (name and address):

Finer Technologies, Inc.

101 Parkview Way, Newtown PA 18940

URL Home site:

<http://www.cyber-sentinel.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
 - File sharing
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
user

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable. (The product is keyword/phrase-based, not category-based.)

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
The behaviour is configurable.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

97%

14. Product description:

- Options
Very configurable, keywords and phrases are programmable and reaction to inappropriate content is configurable.
- Security
Can be installed in stealth or normal mode.
- Technical Requirements (Platform, type of browsers compliant with,...)
Win 98/ME/XP/NT/2000 – IE/NetScape/AOL
- Configuration
/
- Support
Phone/email support available.
- Updates
Updates are free.
- Prices (product, support, updates,..)
\$39.95 – one time only no update fees.
- Extra, useful information about the product / Documentation
/

A.14. Cyber Snoop of Pearl Software Inc.

NAME and version of the product:

Cyber Snoop 5.0

Company (name and address):

Pearl Software, Inc.

URL Home site:

<http://www.PearlSoftware.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Access Monitor

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Web-Mail, Web-Chat, AOL

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
End Users

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporations

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Session ended in case of Chat and IM.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
All data is captured and restored for full analysis.

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
PICS | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?
In function of how products are configured.

14. Product description:

- Options
/
- Security
/
- Technical Requirements (Platform, type of browsers compliant with,...)
All Windows Platforms are supported. Any HTTP, SMTP, POP-3, NNTP, FTP, IRC, IM device.
- Configuration
Handled on client or client Server level.
- Support
A 30 days phone support is available.
- Updates
Life of the product – free.
- Prices (product, support, updates,..)
49.95 US
- Extra, useful information about the product / Documentation
/

A.15. CyberPatrol of SurfControl Inc.

NAME and version of the product:

CyberPatrol – version 6.1

Company (name and address):

SurfControl plc,
Riverside, Mountbatten Way,
Congleton Cheshire CW12 1DY, UK

URL Home site:

<http://www.cyberpatrol.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
 - * Manages access to local programs, i.e. home finance programs etc., and Internet based programs, i.e. P2P file sharing programs, games etc.
 - * With reference to E-mail control, CyberPatrol can filter out offensive text based words and phrases from web based e-mails.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

Cyber Patrol uses a combination of filtering technologies. In addition to using the CyberLIST and CyberPATTERNS, CyberPatrol uses Web Page Analysis technology to interrogate the text and source code of each web page of websites not categorized in our CyberLIST, to enable dynamic categorization of web pages on the fly.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

CyberPatrol's content is sourced using an internal team of over 40 professional researchers, state-of-the-art automated tools, and customer submissions.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses (with small networks of 1–50 PCs).

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD–Rom)
- Guided (Wizard) installation
- Non–guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X–ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

CyberPatrol presently has 9 blocking page styles to choose from, and they are about to release the CyberPatrol Blocking Page Wizard to enable users to create and use their own messages and images to create customized blocking page styles. This helps to create a user/child friendly experience and to meet the needs of individual users/children.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e–mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse–click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Users can review the criteria of our CyberLIST on the website at: http://www.cyberpatrol.com/product/cyberlists.aspx and can test to see if a site is in our CyberLIST by going to our website at CyberPatrol.com and clicking the Test-a-Site link in the top right hand corner of the our home page.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Potentially, it is possible for CyberPatrol to block 100% of unwanted information by using a combination of CyberPatrol's filtering technologies together with the user putting together their own list of unwanted sites. Nevertheless, in reality it has to be recognized that no filtering product is going to block 100% of unwanted content due to the speed of change and dynamic nature of the Internet.

14. Product description:

- Options
Below is a list of features and benefits, for a more detailed list please see the attached pdf of the CyberPatrol Fact Sheet:
 - *Blocks harmful websites and newsgroups
 - *Restricts chat and Instant messaging
 - *Filters Web based e-mail
 - *Manages time online and access to programs
 - *Controls program downloads
 - *Protect personal identity
 - *Customize and fine tune each users filtering settings
 - *Choice of multiple blocking page styles
 - *Quick and easy override of filtering setting
 - *Supports Windows XP fast user switching
 - *'Out-of-the-box filtering
 - *The CyberPatrol 'My Account' provides a secure environment in which users can purchase and manage their CyberPatrol subscriptions.
- Security
 - *There is a secure CyberPatrol HQ logon protecting all users' filtering settings
 - *Each user profile created is password protected.
 - *There's 'out of the box' filtering with a default user profile.
 - *CyberPatrol supports Windows XP's fast user switching and always starts up with the default user profile.
 - *Users cannot bypass CyberPatrol's filtering by deleting files/folders belonging to the CyberPatrol program, changing the system clock, or by manually stopping CyberPatrol processes running.
- Technical Requirements (Platform, type of browsers compliant with,...)

Operating System: XP Pro*/XP Home*/2000 Pro*/Millennium Ed./NT*/98SE

Processor: Pentium II or higher

Memory: 64MB minimum

Disk space: 30MB

Internet Browsers: Microsoft® Internet Explorer 4.0 SP2 and above Netscape 6.0 and above

Internet Connection: A valid Internet connection is required.

*They recommend you have the latest Microsoft® security patch installed.

- Configuration

CyberPatrol 6.1 is even easier to customize and use than ever before. It caters for all types users, whether you are an inexperienced Internet user looking for an 'out-of-the-box' filter, or a power user looking to customize Internet access of individuals or groups of users. Users can also easily immediately implement filtering overrides with no need to restart the computer.

- Support

FREE Technical Support is available to all users around the world of current CyberPatrol products, for more information visit: <http://www.cyberpatrol.com/support/>. From the CyberPatrol website you can download a range of useful 'How To' Guides, check out answers to the most common FAQs, and contact our technical support team by fax or e-mail. Priority Telephone Support is also available and is a chargeable service.

- Updates

There is no extra charge for the CyberLIST updates, and list updates are provided regularly on a weekly basis. Updates are done automatically via the product unless the user chooses to do them manually.

- Prices (product, support, updates,...)

CyberPatrol is provided on an annual subscription basis. A 12 month subscription is USD \$39 / GBP £27 / Euro €39 (excluding local taxes). We also offer a 2 year subscription USD \$69.95 / GBP £49.95 / Euro €69.95 (excluding local taxes) .

The CyberPatrol annual subscription includes:

- CyberPatrol's latest software – with all the top safety and security features
- Weekly updates to our world renowned CyberLISTs
- Free upgrades – both maintenance updates and all major new versions
- Free online, e-mail and fax support

Priority Telephone Support is available 7 days per week and is chargeable (for more detailed information visit – http://www.cyberpatrol.com/support/contact_support.aspx):

Global users – a charge of USD \$9.95 per incident

US users – USD \$1.99 per minute

UK users – GBP £1:00 per minute

- Extra, useful information about the product / Documentation

/

A.16. CyberSitter of Solid Oak Software Inc.

NAME and version of the product:

CYBERSitter

Company (name and address):

Solid Oak Software, Inc.

URL Home site:

www.cybersitter.com

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
 - Server or ISP
 - ISP and User
-

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Standard operating system error messages.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

99 %

14. Product description:

- Options
 - Selectable blocking of WWW, Newsgroups, Chat, Mail, Messaging programs.
 - Detailed log file of user violations.
 - Control Internet access by day and time.
 - Add custom objectionable sites and personal information.
 - Add custom "Always Allowable" sites.
 - Allow access to ONLY specified sites ("White List") if desired.
 - Optional "Family Friendly" search engine redirection.
 - Deny access to TCP/IP ports or port ranges.
 - Ignore access to TCP/IP ports or port ranges.
 - Remote Control program included allows remote configuration.
 - Automatic "Repair" function to fix common problems quickly.
 - Full proxy server support including authentication.
 - Daily activity reports can be sent to parent or administrator by e-mail.
 - User configurable redirection options for blocked sites.
 - Automatic update of filter files performed secretly in the background.
 - New "Suspend" feature suspends filtering for a user defined number of minutes.
- Security
 - Password Protected
 - Sophisticated security and anti-tampering options.
 - Logs unauthorized attempts to access program.
 - Logs attempts to hack program or settings.
 - User selectable stealth options.
 - Optionally disable access to DOS prompt.
 - Optionally disable access to Network control panel applet.
 - Optionally disable access to Internet control panel applet.
 - Optionally disable registry editing.
 - Optionally disable access to the system time applet.
 - Optionally exclude selected user profiles from filtering.
 - Automatic, internal time synchronization with Internet time servers.
 - Automatically disables hacker programs that attempt to alter settings.
 - Dynamic encryption of sensitive settings so that it is different on each computer
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 95/98/Me/NT/2000/XP, Any browser, 3 MB disk space
- Configuration
/
- Support
Free technical support is provided for one full year and is available 7 days a week by e-mail and by telephone during normal business hours. CYBERsitter even has a built in e-mail support function that detects problems and reports them to us so that we can resolve problems quickly and easily.
- Updates
Filter file updates are free and automatically uploaded every 7 days
- Prices (product, support, updates,..)
39.95 single user license, 2-computer \$59.95, 3-computer \$74.95, 5-computer \$99.95, 10-computer \$199.00). There are no recurring fees of any kind
- Extra, useful information about the product / Documentation
/

A.17. dSPAM of Dragon Enterprises

NAME and version of the product:

dSPAM v2.95

Company (name and address):

Dragon Enterprises,
69 St Mildreds Road,
Westgate on Sea, Kent,
CT8 8RL, UK.

URL Home site:

<http://www.dspam.co.uk>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
 - Server or ISP
 - ISP and User
-

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Heuristic analysis

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Themselves as part of the dSPAM service

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Offending emails are deleted or archived.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
Levels of heuristic scanning, trusted list, personal blacklist | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

95%

14. Product description:

- Options
Lite, Standard, Hotmail and Business editions.
- Security
Voluntarily blocks "spam" emails from user.
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 32-bit required, compliant with all POP3 systems plus Hotmail
- Configuration
By user via setup wizard and properties panel.
- Support
By email and fax.
- Updates
In real time via Internet.
- Prices (product, support, updates,..)
Starting from US\$29.99
- Extra, useful information about the product / Documentation
free 15 days trials available

A.18. ENUFF of Akrontech

Unisys

NAME and version of the product:

ENUFF

Company (name and address):

Akrontech

7305 Woodbine Ave.

Suite 620

Markham (Toronto), ON

L3R 3V7

CANADA

URL Home site:

<http://www.akrontech.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Computer Usage Limitor (Type of monitor)

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
Complete access to the computer can be controlled.
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

When the access time for the profile is up, the computer shuts down. No other information is specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Not applicable.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not applicable.

14. Product description:

- Options
No extra options specified on the website.
- Security
The different profiles in ENUFF are password protected.
With the help of many users along the way, Enuff has been refined to be a "bullet proof " product for technological illicit children.
- Technical Requirements (Platform, type of browsers compliant with,...)
Enuff will work under Windows 95, Windows 98, Windows Me, Windows XP (Home and Pro) and Windows 2000.
Any processor
Only 5 Mb of Hard Disk space is needed
The drive A: (floppy disk) should be available for the creation of an emergency disk during installation, but can be provided by company.
- Configuration
ENUFF is configured in 3 easy steps:
STEP 1. Enter up to two Parent/Administrator names and passwords
STEP 2. Enter as many children/user names as you need.
STEP 3. Set the days and times that each user will be allowed to use the computer and Internet.
ENUFF will allow 3 settings per user for example Setting 1 (Mon-Fri), Setting 2 (Sat) and Setting 3 (Sun)
- Support
Akrontech can be contacted by email, telephone or by fax for quick support. On the web site a FAQ – Support page is available as well.
- Updates
For updates to all Windows 9X and Me versions it is free of charge.
There will be a charge for major upgrades (for example, going from ENUFF for Windows 9X or Me to ENUFF XP for Windows 2000/XP) because this is a different program.
Everyone on the user list will automatically be notified about major upgrades. The upgrades can be downloaded via the web site.
- Prices (product, support, updates,..)
One computer (\$34.95)
Two computers (home use) (\$59.95)
Three computers (home use) (\$79.95)
Four computers (home use) (\$89.95)

- Extra, useful information about the product / Documentation
ENUFF is not a filtering program but a kind of monitor and it will not filter out inappropriate websites.
There hasn't been any known conflicts between ENUFF and another filtering program however.

A.19. eTrust Intrusion Detection of Computer Associates

Unisys

NAME and version of the product:

eTrust Intrusion Detection

Company (name and address):

Computer Associates International, Inc.

One Computer Associates Plaza

Islandia, NY 11749, USA

URL Home site:

<http://www3.ca.com/Solutions/Product.asp?ID=163>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

All non-business related categories such as lifestyle, jobs online, jokes, violence, brokers, etc. 27 categories in total.

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector – Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

Offers the ability to detect traffic that violates policy, and automatically terminate the session. This allows the organization to be able to unobtrusively enforce policy with zero impact on performance.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Extended content blocking, the company can define appropriateness of user's surfing behaviour.
Extended and Real Time Monitoring.
- Security
Configuration can only be accessed by administrator(s).
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 98,ME,2000, NT4.0
TC/IP network
- Configuration
Not specified on the website.
- Support
Free technical support in the form of knowledge bases, Faq, forums and personal mail support.
Telephone support is also possible .
- Updates
Free regular updates of products.
- Prices (product, support, updates,..)
No pricing information, prices can be asked via the website.
A free trial version is available online.
- Extra, useful information about the product / Documentation
/

A.20. FilterPak of S4F

Unisys

NAME and version of the product:

FilterPak Business & Education/ FilterPak Home

Company (name and address):

S4F, Inc. 2448 East 91st Street Suite 3900 Tulsa, OK 74137, USA

URL Home site:

<http://s4f.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

The FilterPak works with a list server and a small software program called a "thin-client". Upon installation of the filtering, this "thin-client" is placed on the end-user's computer, where it operates in the background of the system, much like a virus protection program. The "thin-client" requires no further administration or configuration and cannot be turned off or disabled except by the administrator of the account.

The "thin-client" works in concert with the list server by forcing all URL requests to compare against the blocked site list before allowing or disallowing the end-user to view the site. Since this check is merely the comparison of strings of text, it takes a mere fraction of a second to complete.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Alcohol & Tobacco, Drugs, Violence, Gambling, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

- YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
 Estimates indicate that 90 to 99 % of "bad" websites are blocked (92 %)

14. Product description:

- Options
 - Easy configuration
 - Filtering of webpages
 - Configuration of keywords and blackable url's possible
 - Complete monitoring system in Real Time.
 - Security
 - End-users do not perceive the application, FilterPak works as a service, much like an anti virus service.
 - Technical Requirements (Platform, type of browsers compliant with,...)
 - Not specified on the website.
 - Configuration
 - A "Thin-Client" must be installed on the end-user PC's. Configuration occurs online via a website.
 - Each client gets its own personal administration panel online protected with a user name and a password. Easy configuration.
 - Support
 - Online knowledge base / Faq/etc.
 - Tech support is for free.
 - Personal paid support is possible.
 - Updates
 - Updates are generally free if minor changes have been applied.
 - Prices (product, support, updates,..)
 - Filterpak Home ==> \$4.95 per month or \$49.95 per year
 - Filterpak Business & Education ==> Request Quote , use form on website
 - Extra, useful information about the product / Documentation
- /

A.21. Firetrust MailWasher

Unisys

NAME and version of the product:

Firetrust MailWasher Pro 3.3.0

Company (name and address):

Firetrust Limited

Level 2, Strategy Building

374 Montreal St

PO Box 25-297

Christchurch 8001

New Zealand

URL Home site:

<http://www.firetrust.com/products/mailwasherpro/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
EMail Filtering Software (in particular Spam blocking software)

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
User decides the "authenticity" of each received email

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not specified on the website.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Each user of email–software.

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD–Rom)
- Guided (Wizard) installation
- Non–guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X–ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e–mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse–click
- Time logs
- Activities
- Other, please specify:
Not applicable.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: Not applicable.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options

View your e-mail before it gets to your computer, now you see what e-mail is waiting for you so you can deal to it effectively, you can even read the whole message.

Bounce back unwanted e-mail so it looks as if your e-mail address is not valid. This will make the sender think your address is no longer active so your name can be removed from their list. This unique feature is great for privacy and it couldn't be simpler!

Delete unwanted e-mail before you download them. You'll be able to see who the email is from, the subject, and the attachment. This will enable you to decide if you want to delete the e-mail or keep it. A great way to stop viruses or large attachments.

Status. MailWasher Pro analyses each e-mail as it arrives and warns you if it is suspected junk mail or a virus by using fuzzy logic and filtering. The standard status categories are – Virus, Possibly virus, Possibly spam, Probably spam, Blacklisted, Blacklisted by (ORDB, Spam Cop etc). MailWasher Pro even recognises the Klez virus.

Blacklist. Any e-mail you bounce back get their senders details put on the blacklist for easy removal if they come back. You can even set it to automatically bounce and delete blacklisted e-mail, or whole domains off the server. Plus, MailWasher Pro can use external blacklists such as ORDB, Spam Cop, VISI or you can specify your own.

Friends List. Add your friends e-mail addresses to MailWasher Pro and they will always be recognised. You can even hide your friends from the screen so the spam is easy to recognise. Just drag and drop your friends into the friends list.

Filtering. Effective filtering to automatically spot spam, plus it uses a customizable list of blacklisted e-mail senders and/or regular expressions to filter out potential spammer addresses and messages.

Unlimited e-mail accounts. You can have as many e-mail accounts as you want to check. Support for POP3 and Hotmail.

Email overlay. New messages will come in and will reside in the screen until processed.

Fast download of message headers using simultaneous checking, we have clocked speeds of 25 e-mail message headers per second.

Simplicity. No flashy gimmicks, so easy to use that you won't feel like you have to learn a whole new program. In fact it has the familiar look and feel of Outlook Express. It's as easy as 1,2,3. Just check mail, mark for deletion/bounce, then process mail. Plus, MailWasher Pro is only one file, and it won't distribute loads of other files all over your hard drive.

Comprehensive help and frequently asked questions. A tutorial and animated tutorial are also included

Works with your existing e-mail program, whether it is Outlook, Eudora, Netscape or any other program.

- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
Multiple platforms are supported, it runs on Windows 95,98,Me,NT,2000 and XP.
- Configuration
MailWasher Pro is a program with a minimal learning curve, is easy to use and looks attractive.
- Support
First year for free
- Updates
First year for free
- Prices (product, support, updates,..)
Purchase price US\$29.95
- Extra, useful information about the product / Documentation
/

A.22. Freedom Parental Control of Zeroknowledge

Unisys

NAME and version of the product:

Freedom Parental Control

Company (name and address):

Zeroknowledge

Address not specified on the website.

URL Home site:

<http://www.freedom.net/products/parentalcontrol/index.html>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?
- Site labels or rating systems (PICS, an independent rating system)
 - List of URLs
 - Black list
 - White list
 - List of keywords
 - List of keywords combined with analysis of the context in which they appear
 - Analysis of image content
 - Packet analysis
 - Authorization
 - Activity tracing
 - Other, please specify:
Not specified on the website.
5. By whom is the classification of the content done?
- Content providers
 - Third-party experts
 - Local administrators
 - Survey or vote
 - Automated tools
 - Other, please specify:
Not specified on the website.
6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,
- (a) N u d I t y (partial or full)
 - (b) A d u l t p o r n o g r @ p h y
 - (c) C h i l d p o r n o g r @ p h y
 - (d) A n i m a l p o r n o g r @ p h y
 - (e) G r o s s d e p i c t i o n s
 - (f) S e x e d u c a t i o n
 - (g) Other, please specify:
violence, hate, drugs and much more.
7. Which type(s) of public (“buyers”) is targeted?
- Parents
 - Schools
 - ISP
 - Public points of access such as libraries,...
 - Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
Not specified on the website. | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Personal Information Protection
- Security
 - Freedom Parental Control is protected by a unique login system that prohibits children from changing the settings.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Operating System:
 - Windows 98 SE
 - Windows Millennium
 - Windows 2000
 - Windows XP
 - Internet Connection:
 - Minimum 56Kpbs modem or Internet-based connection using standard Microsoft TCP/IP, (A)DSL, Cable modem
 - Hardware:
 - IBM compatible Pentium 233 MHz or higher
 - 64 MB of RAM
 - 15 MB of free hard disk space (minimum installation; 45 MB)
 - Minimum screen resolution; 800x600
 - Browsers:
 - Internet Explorer 5.1 sp2 or higher
 - Mail Clients:
 - Eudora 3.0x, 4.3, 5.1
 - Netscape Messenger 4.x, 6.x
 - Outlook Express 4.0, 5.x, 6.0
 - Outlook 98, 2000,XP
 - Internet Chat & Newsgroup:
 - MIRC 4.x, 5.x
 - Netscape News 4.x, 6.x
 - Outlook Express 4.x, 5.x, 6.0
- Configuration
 - All features are accessible via an easy-to-use user interface. Content filtering levels and access rules can be set to fit your family's particular needs.
- Support
 - Not specified on the website.
- Updates
 - Free automatic updates
- Prices (product, support, updates,...)
 - \$39.95 a year
- Extra, useful information about the product / Documentation
 - /

A.23. IF-2003 of Turner and Sons Production Inc.

Unisys

NAME and version of the product:

The Internet Filter IF-2003

Company (name and address):

Turner and Sons Production Inc.

151 - 56 Dunbar St.

Vancouver B.C. V6S 2C2

Canada

telephone/fax 604-708-2397

URL Home site:

<http://www.turnercom.com/if/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Using a white list of url's other pages are blocked (user dependable)

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Workplace

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
This program is crossplatform filtering software to be configured for either the client, proxy server, or ISP server level
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
Works with client, proxy server, and ISP server for Windows 2000 & NT, all linux systems as well as NetBSD and Mac OS-X .
- Configuration
Configuration occurs via the administration panel relatively easy (Web application).
- Support
On the website, only email addresses are provided.
- Updates
The costs of the updates of the filtering product depends on how many systems in use, for detailed explanations take a look at <http://www.internetfilter.com/coompetitive.html>
- Prices (product, support, updates,...)
Price depends on how many systems in use, for detailed pricing take a look at <http://www.internetfilter.com/pricing.html>
- Extra, useful information about the product / Documentation
/

A.24. I-Gear of Symantec Corporation

Unisys

NAME and version of the product:

I-Gear

Company (name and address):

World Headquarters

Symantec Corporation

20330 Stevens Creek Blvd.

Cupertino, CA 95014

tel +1 408 517 8000

URL Home site:

http://www.symantec.com/sabu/igear/igear_educ/features.html

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

All categories are possible – It's up to administrator to configure

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Powerful Access Scheduling is available.
Complete reporting functionalities are available.
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - I-Gear for Windows NT
 - PC Based on an Intel® Pentium® or compatible processor, with 64MB RAM, CD-ROM Drive
 - 25MB available disk space for software, plus 200MB (>1GB recommended) for cached data
 - Internet access and World Wide Web Browser (suitable browsers include Netscape Navigator 2.0 or later or Microsoft Internet Explorer 3.0 or later)
 - Microsoft Windows NT Server 4.0 with Service Pack 3 or later installed
 - I-Gear for MS Proxy
 - PC based on an Intel® Pentium® or compatible processor, with 32MB RAM, CD-ROM drive
 - 30MB available disk space
 - Microsoft® Windows NT Server Version 4.0, with Service Pack 3 and Internet Information Server 3.0
 - Microsoft Proxy Server version 1.0 or 2.0
 - Internet access
 - I-Gear for Solaris
 - SPARC™-based system, 64 MB RAM, CD-ROM drive
 - 30MB disk space for software
 - 400MB (1GB recommended) for cached data
 - 50MB for log files
 - 10MB for settings files
 - Solaris™ 2.5 or later, or Netra™i 3.1
 - Internet access
 - I-Gear for Linux
 - PC Based on an Intel® Pentium® or compatible processor, with 64MB RAM, CD-ROM Drive
 - 25MB available disk space for software, plus 200MB (>1GB recommended) for cached data
 - Internet access and World Wide Web Browser (suitable browsers include Netscape Navigator 2.0 or later or Microsoft Internet Explorer 3.0 or later)
 - Red Hat Linux 5.2 or 6.0
- Client Requirements

- Any CERN HTTP Proxy protocol compliant browser such as – Microsoft Internet Explorer™ version 3.02 or later – Netscape Navigator™ version 2.0 or later.
- Configuration
Not specified on the website.
- Support
Free online support for customers (guides, knowledge base, faq,..)
Fee based "personal" technical support (\$29.95 per incident, 6:00 A.M. to 5:00 P.M. PT Monday through Friday)
- Updates
Product updates are not free but must be purchased.
- Prices (product, support, updates,..)
The price list can be requested by Symantec.
- Extra, useful information about the product / Documentation
/

A.25. Internet Sheriff of Tel.net Media

Unisys

NAME and version of the product:

Internet Sheriff

Company (name and address):

Tel.net Media Europe

Atlantic House

Imperial Way

Reading

RG2 0TD UK

URL Home site:

<http://www.telnetmedia.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
 - Incidence of indicative words or phrases in the body text of the website
 - Incidence of unique occurrences of indicative words or phrases in the body text of the website
 - Ratio of indicative words or phrases to the overall significant text content of the website
 - Incidence of indicative words in the domain name of the website
 - Incidence of indicative words or phrases in the 'keywords' content of the meta-information element of the header section of the website
 - Ratings service category values including Safe-Surf™, Recreational Software Advisory Council, EvaluWEB™ etc
 - Incidence of images by size and quality
 - Ratio of graphical to total website content
 - Incidence of files with audiovisual formats
 - Incidence of indicative words or phrases in alternative text associated with objects on the website
 - Incidence of links to known sites of the same classification

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

The complete list can be found at:
<http://www.telnetmedia.com/products/inetsheriff/index.php?page=cat>

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
/
- Security
Access attempts by users to internet content can be blocked, allowed or logged according to the content category, content-type (MIME) or file extension of the internet material being examined.
- Technical Requirements (Platform, type of browsers compliant with,...)
Following hardware platforms and systems are supported:
SOLARIS :
Sun Sparc architecture ==> Sun Solaris 87 or higher 256MB Ram,512MB recommended.
Intel x86 architecture ==> Sun Solaris 8 or higher, 256 MB Ram but 512 MB recommended.
LINUX :
Intel i386 architecture (minimum) ==> 300 MHZ,128MB (minimum) Redhat 6.X
Intel i686 architecture (ideal) ==> 1GHZ, 512MB Ram, SMP Kernel 2.4.8 - 2.4.16, Redhat 7.X/Mandrake 8.X
- Configuration
Internet sheriff comes with a controlled user internet environment that works via a point-and-click web-based interface, from any workstation or desktop computer connected to the internet.
- Support
Customers get free personalised email and phone support.
Online help libraries are available.
- Updates

- Not specified on the website.
- Prices (product, support, updates,..)
For pricing info, contact sales@telnetmedia.com.
- Extra, useful information about the product / Documentation
/

A.26. iWayPatrol of iTECH Inc.

Unisys

NAME and version of the product:

iWayPatrol (different versions for school, libraries, corporate sector) / iWayMail

Company (name and address):

iTECH Inc.

6601 Washington Avenue

Racine, WI 53406

(262) 884-8562 or (800) 523-4795

(262) 884-8761 fax

URL Home site:

<http://www.itech-mke.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
 - Self labelling tags (RSACi, Safe for Kids, and Safe Surf);
 - DNS analysis and pattern matching
 - Contextual analysis of web page language.. (to avoid "overblocking")

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
 - Alcohol, Chat, Drugs, Gambling, Games, Illegal activities, Jobs, Jokes, Personals, Shopping, Tobacco, and many others ..==>See http://www.itech-mke.com/itech_category.html for complete list

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

A user attempting to access a blocked web site is given a notice that the site is not available. A user adding a News group via the browser is given a choice of news groups which does not include the gaming and sex related sites

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> ·local control permits administrators to add and delete individual sites from blocking lists. ·local control permits administrators to add and delete filter categories i.e. Games. (For more information on categories.) ·local control permits administrators to adjust content pattern lists. ·local control permits administrators to adjust RSACi and SafeSurf self labelling codes blocking values. <p>==> iWayPatrol allows customized blocking. One alternative is the option of restricting Internet access to only selected sites. (http://www.iwaypatrol.com/admin/admin_index.html)</p>		

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
Server Based system (Combination of hardware and software)
Own hardware can be used, in this case only software licenses must be acquired.
System Hardware: The iWayPatrol filter is available on three standard platforms forms:
 - iTECH Intel Filter Server (Celeron or Pentium)
 - iTECH Qube Filter Server (Cobalt or Gateway)
 - iTECH Sun Filter Server (Netra X1 or Sun Blade)
- Configuration
Adding additional sites to block; deleting sites from the blocking list; adding News groups; deleting news groups; maintaining local blocking and filtering lists are all easily maintained through a series of administrative browser screens by the IS manager. Installation of the operating system software, the filter software, proxy software takes an estimated 4 to 8 hours.
- Support
Is provided -- On site installation and training support takes 6 to 10 hours. The iTECH standard service rates apply. Interfacing the administrative computer data base to generate the names and password can take 8 to 16 hours.
- Updates
NewsNet and Site Blocking Lists are updated via the Internet on a weekly basis by iTECH staff. Local backup can be performed to maintain the local parameter and local blocking lists.

The monthly maintenance fee is scaled to the number of Internet computers on the filter network. The monthly fee covers updates to the software. As improvements are made subscribers receive updates with the additional features available.

- Prices (product, support, updates,..)

Since the size, growth, needs and existing network of each customer are unique, a quote based on some additional information is necessary..

In general :

1. Software License Fee: The license fee is a one time, flat fee which includes the software, the proxy software as necessary, and the use of the software on one computer. The license fee is scaled to the size of the district and features. Generally the prices range from \$999 to \$3,500.

2. System Hardware: The iWayPatrol filter is available on three standard platforms forms:

- iTECH Intel Filter Server (Celeron or Pentium)
- iTECH Qube Filter Server (Cobalt or Gateway)
- iTECH Sun Filter Server (Netra X1 or Sun Blade)

Price is dependent on speed, size and configuration required for the expected number of users. Generally the prices range from \$1,250 upward. Custom systems are available for larger Districts. Hardware can be optionally provided by the client.

- Extra, useful information about the product / Documentation

/

A.27. KidSafe Explorer of Arlington Software

Unisys

NAME and version of the product:

KidSafe Explorer

Company (name and address):

Arlington Software

329 Great Eastern Highway

Redcliffe, WA, 6104

Australia

Tel: +61 403 456721

URL Home site:

<http://www.arlington.com.au>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
 - Prevents popup windows
 - Prevent launching of other programs

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Apart from restricted site access, some of the other configurable options include logging of web sites accessed, prevention of file downloads and the ability to customise the toolbar and include your own logo.
- Security
The parent is prompted to enter an admin password when running KSE for the first time . This allows parents to control who can access the Options area where various restrictions are defined. KSE can prevent other browsers from running, in order to prevent unmonitored surfing.
- Technical Requirements (Platform, type of browsers compliant with,...)
Internet Explorer must be present on the PC (and is built into Windows), but you do not need to run IE in order to use KSE.
- Configuration
Occurs via the "options menu", very simple point to click tab system where all options can be configured
- Support
Knowledgebase on the website (FAQ, Guides, Known problems,)
Mail support for customers
- Updates
Once registered, all subsequent "point one" upgrades are free. For instance, upgrading from v8.0 to v8.1 is free, but there will be a fee for upgrading to version 9.0
- Prices (product, support, updates,...)

1 – 9	\$35 per PC
10 – 19	\$32 per PC
20 – 49	\$29 per PC
50 – 99	\$26 per PC
100+	\$22 per PC
- Extra, useful information about the product / Documentation
/

A.28. KidsNet

Unisys

NAME and version of the product:

KidsNet

Company (name and address):

Kidsnet, Inc.

2002 San Marco Blvd, Suite 201

Jacksonville, FL 32207

USA

URL Home site:

<http://www.kidsnet.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

100% reviewed by people / no artificial means of filtering/blocking.

Kidsnet reviews Web sites based on the Internet Content Rating Association (ICRA) standards plus content rating standards developed by Kidsnet.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Kidsnet is a parental control system exclusively based on human reviewers.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

22 individual categories ==> <http://www.kidsnet.com/rescat.asp>

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Nice graphic explaining the kid that there might be "pirates on the route" and providing other more useful links.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Parents can send a request to a Kidsnet reviewer.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Parents may prevent all applications from reaching the Internet
Parents may prevent executable files from being downloaded from the Internet.
Controls and settings remain even if the child uses the product on another computer.
- Security
Once your Kidsnet software has been downloaded, you may set up individual accounts for each of your children. These accounts will be the same on all the computers on which you install Kidsnet. Your children's Internet access is allowed only by means of a password you assign to each child. Kidsnet ensures that any time your child uses a computer, he will see only what you consider appropriate.
- Technical Requirements (Platform, type of browsers compliant with,...)
Not specified on the website.
- Configuration
The Control Room allows to fine tune the settings for a child's individual needs.
- Support
Knowledgebase (Faq, guides, ..) and free email support is available.
- Updates
Kidsnet can currently respond to requests in less than 24 hours. The kidsnet process included an automatic request when a Parent attempts to access a site not in the Kidsnet database AND an expedited request feature.
- Prices (product, support, updates,..)
A Subscription to Kidsnet is \$40.00 per year. A one year subscription gives access to the ever-changing and constantly updated Kidsnet universe of Websites and Priority next business day e-mail support. The price includes settings for up to 6 child accounts and access to the Kidsnet Internet for 365 days. Kidsnet comes with a 30 day money back guarantee.
- Extra, useful information about the product / Documentation
Kidsnet offers www.hazoo.com, a search engine for child friendly Web sites.

A.29. Kidweb

Unisys

NAME and version of the product:

Kidweb

Company (name and address):

Not specified on the website.

URL Home site:

<http://www.email-connection.com/KWFINAL.html>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

All categories are configurable

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Access to the browser is secured with a user/password system. The user profiles loads automatically after logging in.
- Technical Requirements (Platform, type of browsers compliant with,...)
A personal computer with an 80486 processor (or higher).
Microsoft Windows version 3.1 (or higher).
At least 8 MB of RAM.
MS-DOS version 3.1 or later (MS-DOS 5.0 or newer recommended).
From 9 – 15 MB available hard disk space, depending on the type of installation you choose.
- Configuration
Easy configuration for new computer users via Parental Control Panel.
- Support
Knowledge base online, mail and www support are free for customers.
- Updates
Updates are for free.
- Prices (product, support, updates,...)
"Not available at this time" (as seen on their website)
- Extra, useful information about the product / Documentation
/

A.30. Kidz.net of Kidz.net National Pty. Ltd.

NAME and version of the product:

Kidz.net

Company (name and address):

Kidz.net National Pty. Ltd.

URL Home site:

<http://www.kidz.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

Not applicable since only white list approach is used.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|--------------------------|-------------------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Kidz.net uses a whitelist technology. The degree of blocking can be controlled at the proxy or at the browser by parents. Parents can choose to unblock the sites blocked by Kidz.net.

14. Product description:

- Options
2 types of products: Proxy-based or client-based
- Security
White list based. Also using WinSOCK to detect Internet-related traffic.
- Technical Requirements (Platform, type of browsers compliant with,...)
Proxy: Linux Red Hat with SQUID.
Client-based: Windows platforms – Internet Explorer-based browser.
- Configuration
Server: Microsoft SQLserver + Coldfusion; Client based: Java + Visual Basic
- Support
Only 2-tier support. 9–5 Mon–Fri.
- Updates
Each year an update is provided.
- Prices (product, support, updates,..)
For pricing info, please contact Kidz.Net directly.
- Extra, useful information about the product / Documentation
Contact Kids.Net for further information on (02) 9428 8924.

A.31. Line-Loc

Unisys

NAME and version of the product:

LineLoc

Company (name and address):

Line-LocTM Ethel Court Grayling, MI 49738

URL Home site:

<http://members.tripod.com/~lineloc/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
A Hardware Lock used to "lock" a phone or internet line.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Can put internet on or off.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Not applicable.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not applicable.

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Other, please specify:
Not applicable. | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not applicable.

14. Product description:

- Options
Line-LocTM is a simple hardware solution that gives parents total control over Internet time.
This device is also a convenient way for parents to control when kids are spending too much time online.
- Security
It is very simple to understand, once the key is turned off all the passwords in the world will not get that computer online until the key is turned back on.
- Technical Requirements (Platform, type of browsers compliant with,...)
Not applicable.
- Configuration
It is very simple to understand, once the key is turned off all the passwords in the world will not get that computer online until the key is turned back on.
- Support
Not applicable
- Updates
Not applicable.
- Prices (product, support, updates,..)
\$17.95 + \$2.95
- Extra, useful information about the product / Documentation
/

A.32. MailWasher

Unisys

NAME and version of the product:

MailWasher Free / Mailwasher Pro

Company (name and address):

MailWasher

Level 2, Strategy Building

394 Montreal St

P.O.Box 4620

Christchurch 8015

New Zealand

URL Home site:

<http://www.mailwasher.net/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Spam filter

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Analysis of incoming emails and blocks them if it is suspected junk mail or a virus by heuristic checking and filtering.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
All Spam and unwanted emails

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
All email users

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not applicable.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: The blacklists of emailoriginators and the whitelists can be reviewed and modified.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Bounce e-mails
 - Delete e-mails
 - Analyse e-mails
 - Blacklist
 - Friends list
 - Access external DNS spam blacklists
 - Filters
 - New easy to use interface (only Pro version)
 - Drag and drop e-mail addresses (only Pro version)
 - Highlighted grid lines for easy reading(only Pro version)
 - Hotmail access(only Pro version)
 - Technical support (only Pro version)
 - Affiliate program (only Pro version)
 - Access global spam database (only Pro version)
- Security
 - Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - 4 Mb of RAM, 4Mb of disk space, and an Internet connection.
 - Runs on Win95 / 98 / Me / NT4 / 2000 / XP / XP Pro
 - MailWasher works independently of other email programs so it doesn't matter which one you use.
- Configuration
 - Very easy configuration panel.
- Support
 - Technical support is only possible for the Pro version free of charge.
- Updates
 - Not specified on the website.
- Prices (product, support, updates,..)
 - MailWahser is Free
 - MailWasherPro : 29.95\$
- Extra, useful information about the product / Documentation
 - /

A.33. Maranatha Filter

Unisys

NAME and version of the product:

Maranatha Filter

Company (name and address):

Address isn't specified on the website

URL Home site:

<http://www.maranatha.net/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Maranatha filters can work with any ISP and are provided as a service.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
extreme violence, witchcraft, hate sites, building bombs, and others

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |
| None of the above. | | |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Maranatha offers a “forced” system, which cannot be disabled by a user. Customers wishing to take advantage of the filtration technology, but on an elective basis, can select the “unforced” option. This provides all the benefits of the technology when you want it, but allows you to disable the filter when needed, e.g. when engaged in academic or medical research etc.
- Technical Requirements (Platform, type of browsers compliant with,...)
Just a computer with Internet access.
- Configuration
Configuration for ISPs is not specified on the website.
User configuration isn't necessary.
- Support
Phone and mail support are provided.
- Updates
Maranatha constantly updates the database.
- Prices (product, support, updates,..)
Maranatha Filter only (no dial up access) \$5.00 /month
- Extra, useful information about the product / Documentation
/

A.34. MoM of A. Value Systems

Unisys

NAME and version of the product:

MoM

Company (name and address):

A.Value Systems

P.O.Box 163

Keene, NH 03431

URL Home site:

<http://www.avswweb.com/mom/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Web Monitor for Tracking Children or Employees Online

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not specified on the website.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not specified on the website.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Other, please specify:
Not specified on the website. | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Not specified on the website.
- Security
MoM can run in "stealth" mode, users won't even notice they are being watched and monitored.
- Technical Requirements (Platform, type of browsers compliant with,...)
MoM runs best on a WIN95 (not NT) computer
with a Pentium 200mhz or faster* processor,
24mb of RAM, 20mb of free hard disk space,
and MORE than 256 color video.
- Configuration
Not specified on the website.
- Support
MoM's technical support is all handled by email. FAQs and online guides are present.
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
20 \$
- Extra, useful information about the product / Documentation
/

A.35. N2H2 of Secure Computing

Unisys

NAME and version of the product:

N2H2

Company (name and address):

Secure Computing Corporate Headquarters

4810 Harwood Road

San Jose, CA 95124-5206

UNITED STATES

Toll Free: 800-692-5625

Tel: 408-979-6100

Fax: 408-979-6501

Sales & Service: 800-379-4944

URL Home site:

<http://www.n2h2.com.au>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
By Specialised People working for Secure Computing.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Hacking, Gambling, Drugs, Extreme violence, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Workplaces

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not specified on the website.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

98%

14. Product description:

- Options
The features available are listed on <http://www.n2h2.com.au/products/bess.php?device=features#rpt>
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
P2 300MHZ with 512MB Ram and 6GB HD Space
Appliances supported by N2H2:
 - Cisco Routers
 - Cisco Pix Firewall
 - Cisco Content Engine
 - Novell Border Manager
 - Microsoft ISA
 - Microsoft Proxy 2
 - Sonic Wall
 - Checkpoint Firewall
 - Stratacache
 - Volera Excelerator
- Configuration
Very easy to install and configure while offering a good level of granularity in setting security policies and options.
- Support
Online support : Web- based and active discussion forums
Tech Support via phone, fax and email is provided to customers.
- Updates
Not specified on the website.
- Prices (product, support, updates,...)
5\$ per year per user for large installations, 25\$ /year/user for small ones
- Extra, useful information about the product / Documentation
/

A.36. Net Guardian of Maximum Internet Limited

Unisys

NAME and version of the product:

Net Guardian

Company (name and address):

Maximum Internet Limited

PO Box 8006

Symonds Street

Auckland 1035

New Zealand

URL Home site:

<http://www.maxnet.co.nz>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
- Conventional proxy application
- Transparent proxy application
- Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
TCP Port blocking
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Net Guardian utilises an array of powerful, high-speed computers called the "Mudcrawler" that visit Internet sites in search of specific criteria. The sites that meet the criteria are then viewed by a team which decide if the site should be blocked or not. This means that legitimate sites, such as medical sites, are not blocked.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

Anarchy,Cults,Drugs,Free Hosts,Gambling,Hate and Discrimination,Illegal activity,Obscene & Tasteless

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector, Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not specified on the website.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Not specified on the website.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Password protected interface for the users.
- Technical Requirements (Platform, type of browsers compliant with,...)
No extra user installation required, everything occurs on Maxnet's network.
- Configuration
The Net Guardian server is located on Maxnet's network, standing between you and the Internet. Net Guardian checks every website request against a library of website addresses, and blocks it if the site is found in the library.
See http://www.8e6.com/products/R3000/pd_r3000_how.htm and
http://www.8e6.com/products/R3000/pd_r3000_feats.htm
- Support
Standard technical support is available to 8e6 customers 6am-5pm PST Mon-Fri through the support staff. 24/7 support options are also available. Additional help, technical support and documentation are also available online.
- Updates
Net Guardian's library system is updated daily with approximately 8000 new websites and the current library lists several million web pages.
Net Guardian uses an R2000 server with automatic daily updates and seamless integration for a client.
- Prices (product, support, updates,..)
For pricing info, take a look at <http://www.maxnet.co.nz/content/netguardian/19/168/515.htm>
- Extra, useful information about the product / Documentation
/

A.37. Netfilter of nXp Technologies

Unisys

NAME and version of the product:

Netfilter 4.1

Company (name and address):

nXp Technologies

711 Louisiana Street

Suite 1740

Houston, Texas 77002

URL Home site:

<http://www.nxp.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Dynamic Filtering

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

The categories are configurable.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

When an employee requests a site that is restricted, the netFilter Blocking Page is generated. Blocking Pages can also be configured to show only a logo and a message from the company, making the netFilter v4.1 presence transparent to the employees.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Server-based
 - Database of Sexually-Explicit Adult Web Sites Updated Daily
 - Dynamic Filter
 - Database Content Modification
 - URL Monitoring and Analysis Interface
 - Frequent URL Caching System
 - Scaleable
 - Plug-and-Play Workstation Configuration
 - Allows transparent filtering
- Security

As a Server Based filter, netFilter v4.1 is installed at the central network location by a network administrator. Since netFilter v4.1 works as part of a local network's normal Internet routing, it is effective throughout the entire network and cannot be circumvented at the desktop computer level. With netFilter v4.1, no other software is necessary.
- Technical Requirements (Platform, type of browsers compliant with,...)

The following server systems are netFilter v4.1 compatible:

 - Linux 2.0 (80x86)
 - Linux 1.2.13 (80x86)
 - Linux 2.0 PPC (PowerPC)
 - Debian GNU/Linux 1.3 (80x86)
 - Red Hat Linux 4.0 and above (80x86)
 - BSDI 3.0 (80x86)
 - Free BSD 2.1 (80x86)
 - Solaris x86 2.5.1 (80x86)
 - Solaris 2.5.1 (sparc)
- Configuration

Because netFilter v4.1 offers Transparent Filtering, one doesn't have to preconfigure each workstation's Internet browser proxy preferences. When netFilter v4.1 is configured at the network level, it will accept Internet inquires from all the connected workstations, independent of whether the browsers are set correctly or not.
- Support

Support will always be given by someone who speaks your language and by someone who understands your needs.
- Updates

Not specified on the website.
- Prices (product, support, updates,..)

Not specified on the website.
- Extra, useful information about the product / Documentation

Due to workload pressures on a limited staff, many network managers prefer to purchase a workstation that contains the filtering software and its operating system already preconfigured. This way, all one has to do is "plug" the workstation into the network and turn it on. With Plug-and-Play

Workstation Configuration available, the UNIX-based filter can be sold to customers with NT- or Mac-platform networks.

A.38. NetIQ WebMarshal of Ancoris Limited

Unisys

NAME and version of the product:

NetIQ WebMarshal

Company (name and address):

Ancoris Limited

Knyvett House

Watermans Business Park

The Causeway

Staines, TW18 3BA

URL Home site:

<http://www.ancoris.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Lexical Scanner

WebMarshal uses an advanced lexical scanning engine to review the text of web pages as they are retrieved. The scanner searches the text for the presence of keywords you specify in search scripts. Based on the result of the scan, web pages or sites may be placed on a blacklist or whitelist which will determine future access. This occurs without affecting the user's browsing experience. Scripts may include wildcards and boolean combinations of words (using AND, OR, NOT, NEAR, FOLLOWEDBY). Each script may include many conditions.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

All categories possible

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate Sector , workplace

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

WebMarshal logs all web requests, whether successful or rejected. From these logs, a comprehensive range of reports and graphs can be generated – by user, by site, by bandwidth, by browsing time, etc. These reports will be useful for setting company policy or even for internal charging purposes.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Standalone Proxy Server for HTTP, HTTPS and FTP (non-caching).
 - Supports Web Filter plugin installation on Microsoft ISA Server, and chaining to other proxy servers.
 - Supports filtering by Windows NT login, Novell NDS login, or workstation.
 - Allows virus scanning of file downloads and uploads.
 - Quota Rules allow browsing to be limited by total time or bandwidth per user.
 - Site Rules allow browsing control by URL, user, and time of day.
 - Content Download Rules allow browsing control by file type, size, and virus scanner results.
 - TextCensor Rules allow automated local updating of site blacklists and whitelists (URL Categories).
 - Content Upload Rules provide control of file uploads by site, content and TextCensor criteria.
 - Uses Marshal's TextCensor lexical analysis technology to categorize pages.
 - Allows virus scanning of file downloads and uploads.
 - Quota Rules allow browsing to be limited by total time or bandwidth per user.
 - Site Rules allow browsing control by URL, user, and time of day.
 - Content Download Rules allow browsing control by file type, size, and virus scanner results.
 - TextCensor Rules allow automated local updating of site blacklists and whitelists (URL Categories).
 - Content Upload Rules provide control of file uploads by site, content and TextCensor criteria.
 - Uses Marshal's TextCensor lexical analysis technology to categorize pages.
 - Allows stripping of "cookies"
 - Administrators can monitor pages requested by user in real time.
 - Provides Windows NT Performance Counters.
 - All requests are logged and a wide variety of reports can be generated.
- Security

WebMarshal may be configured to check upload and download file content using a third-party anti-virus product. Based on the results of the virus check, the upload or download may be blocked. This function will be particularly useful in checking attachments to Web-based email.
- Technical Requirements (Platform, type of browsers compliant with,...)

Webmarshal :

 - Pentium II 400 Mhz 512 MB RAM ,1 GB Harddisk space
 - Windows 2000 or later, MSQlServer 7.0 or 2000

Administration Console :

 - Pentium II 166 Mhz 128MB Ram, 5 MB Harddisk space
 - Windows 2000 or later
- Configuration

You can install WebMarshal:

- on a separate server with an existing proxy server
- on an existing proxy server
- on a Microsoft ISA server configured as a proxy server
- Support
Telephone and email support are available.
- Updates
Not specified on the web site.
- Prices (product, support, updates,..)
Prices are not supplied. Please contact the sales departement for a detailed quote.==
><http://www.ancoris.com/forms/quotereq.asp>
- Extra, useful information about the product / Documentation
/

A.39. NetNanny of BioNet Systems

Unisys

NAME and version of the product:

NetNanny 5

Company (name and address):

BioNet Systems, LLC

1605 NW Sammamish Road, Suite 105

Issaquah, WA 98027

ph: 425-649-1100

fx: 425-649-1110

URL Home site:

<http://www.netnanny.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
 - Blocks popups
 - Blocks other internet related software on the user PC.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not specified on the website.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Violence, Racism and many more.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Blocks cookies
 - Emailed activity report
 - Blocks most pop-up windows
 - Blocks internet enabled applications
 - etc
- Security

All user settings are password protected. Children can not access other internet related applications if chosen so by the administrator (parents).
- Technical Requirements (Platform, type of browsers compliant with,...)

Net Nanny 5 has been designed to work on any PC you may use from home or work. (Windows, Internet explorer or Netscape) In their latest release, they have added support for the latest Internet technologies, including popular web browsers, instant messenger applications, and file trading programs.

Net Nanny 5 works with all major ISPs, including dial-up modem connections, cable modems, DSL, and other high-speed Internet access technologies. Performance will vary depending on your computer's speed, your connection speed to the Internet, and other factors.

Net Nanny 5 is not compatible with Windows 95 neither with Apple Macintosh.
- Configuration

For installation on user PCs, Wizard like screens for easy configuration are available. By clicking on a shortcut button, the system displays the corresponding system setting.
- Support

FREE Technical Support. Net Nanny offers email and website support to registered users all over the world. From their web site (netnanny.com), one can download user manuals and get solutions to common problems. Contact technical support by e-mail or by using the feedback form.
- Updates

The cost to upgrade is \$14.95 USD for all registered Net Nanny customers.
- Prices (product, support, updates,..)

€39.95 for single download

Prices for Net Nanny 5 on multiple computers start at under EUR 35.00 for Download and are discounted by volume.
- Extra, useful information about the product / Documentation

/

A.40. Netprotector of The Modem Lock Company

Unisys

NAME and version of the product:

Netprotector

Company (name and address):

The Modem Lock Company

P.O. Box 1658

Framingham, MA 01701

URL Home site:

<http://www.modemlock.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Very simple Hardware Lock used to "lock" a phone or internet line.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Can put internet on or off.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Not applicable.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not applicable.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: Not applicable.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not applicable.

14. Product description:

- Options
Line-LocTM is a simple hardware solution that gives parents total control over Internet time. Its inexpensive and very simple to understand. Once the key is turned off all the passwords in the world will not get that computer online until the key is turned back on. This device is also a convenient way for parents to control when kids are spending too much time online.
- Security
Not applicable.
- Technical Requirements (Platform, type of browsers compliant with,...)
Not applicable.
- Configuration
Not applicable.
- Support
Not applicable.
- Updates
Not applicable.
- Prices (product, support, updates,...)
\$17.95 + \$2.95
- Extra, useful information about the product / Documentation
/

A.41. Norton Internet Security of Symantec Corporation

Unisys

NAME and version of the product:

Norton Internet Security 2004

Company (name and address):

Symantec Corporation

20330 Stevens Creek Blvd.

Cupertino, CA 95014

tel +1 408 517 8000

URL Home site:

http://www.symantec.com/sabu/nis/nis_pe/features.html

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Anti Virus, Anti Spam, Firewall and Privacy Control

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Block internet enabled applications on user pc

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
 - Security monitor
 - Spam alert
 - Visual attack tracking
 - Password protection
 - Internet privacy control
 - etc
- Security
 - All configurations occur at administration level that is Password protected.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Windows® XP Home Edition/Professional
 - 300MHz or higher processor
 - 128 MB of RAM
 - Windows 2000 Professional
 - 133MHz or higher processor
 - 96 MB of RAM
 - Windows Me
 - 150MHz or higher processor
 - 96 MB of RAM
 - Windows 98
 - 133MHz or higher processor
 - 64 MB RAM
 - REQUIRED FOR ALL INSTALLATIONS
 - 200 MB of available hard disk space
 - DVD or CD-ROM drive
 - Internet Explorer (minimum version 5.01 SP2 required)
 - Email scanning supported for standard POP3 and SMTP compatible email clients.
 - Supported instant messaging clients for virus scanning:
 - AOL® Instant Messenger (minimum version 4.7 required)
 - Yahoo® Instant Messenger (minimum version 5.0 required)
 - MSN® Messenger (versions 4.6, 4.7)
 - Windows® Messenger (minimum version 4.7 required)
 - Supported instant messaging clients for private information blocking:
 - AOL Instant Messenger (minimum version 4.3 required)

- Yahoo Instant Messenger (minimum version 5.0 required)
- MSN Messenger and Windows Messenger (minimum version 3.6 required)
- Configuration
Configuration occurs via easy wizard like panels . Each component of Norton Internet Security has its own application to configure.
- Support
Knowledge bases, downloads, contact options.
- Updates
One year of protection updates included with purchase of Norton Internet Security 2004; annual subscription available for subsequent updates.
- Prices (product, support, updates,..)
\$69.95
- Extra, useful information about the product / Documentation
/

A.42. Optenet

Unisys

NAME and version of the product:

OPTENET

Company (name and address):

OPTENET

Parque tecnológico de Miramón – Edificio B8

Paseo Mikeletegi 58– 1ª planta

20009 San Sebastián

URL Home site:

<http://www.optenet.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
(one PC and one Server version)

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Racism, sects, drugs, terrorism, anarchy.

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

97%

14. Product description:

- Options
On their website, a range of options is mentioned.
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
The PC version is distributed for Windows 95/98/ME/NT/2000/XP and it can be used jointly with any Internet Browser, such as Netscape Navigator or Internet Explorer (Pentium compatible , 32MB Ram)
Server Version :
Windows NT, Windows 2000 SERVER: OPTENET operates on these platforms as a Microsoft Proxy plug-in, using the ISAPI interface. OPTENET also operates on these platforms as a plug-in of the Inktomi Traffic Server.
Linux: OPTENET operates in Linux as an added module of Squid.
Solaris: OPTENET operates in Solaris as an added module of Squid. OPTENET also operates on this platform as a plug-in of the Inktomi Traffic Server.
- Configuration
OPTENET has an installation wizard incorporated that enables easy installation. It informs the user of the process step by step and requests the information that is required.
- Support
Free phone help-line
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
* Pc Version : 39 euros
* All other versions : contact sales department for detailed quote.
- Extra, useful information about the product / Documentation
/

A.43. Perkeo++ of AUTEM GmbH

Unisys

NAME and version of the product:

Perkeo

Company (name and address):

AUTEM GmbH

Dithmarscher Straße 13

D-26723 Emden

URL Home site:

<http://www.perkeo.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

PERKEO[®]++ is a data scanner, which assists you to locate child illegal child-pornography and animal-pornography. PERKEO[®]++ gives you the possibility to scan for such objects.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

PERKEO++ doesn't look out for personal data, it only makes a pure comparison of calculated digital fingerprints with reference values of a PERKEO[®]++ database.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

PERKEO^{®++} creates of each file a digital fingerprint and compares it with the entries of a PERKEO^{®++} database. Each database includes digital fingerprints of one logical area.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Not applicable.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

Currently the following databases for PERKEO^{®++} are available:
against child pornography and animal pornography (each can be deactivated).

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
An automatic message to criminal investigation departments can be generated.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Not applicable.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: Not applicable	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

The used algorithm to calculate the fingerprints has an error rate of less than 1 : 1034 which makes PERKEO®++ 100 percent secure in practice.

14. Product description:

- Options
 - Extremely fast. Results of more than 100 MB/s are possible
 - PERKEO®++ works on any local drives (hard discs, CD-ROM, Floppy ...) and network drives
 - PERKEO®++ scans compressed archives (ARJ, ZIP)
 - Scanning of usenet News (also DNEWS)
 - Scanning of Webspaces
 - Scanning of Proxy-Cache
 - 100% accuracy in practice
- Security
Not applicable.
- Technical Requirements (Platform, type of browsers compliant with,...)
Following OS are supported :
 - DOS/Win95/98/NT
 - AIX 4.2 (PowerPC)
 - DEC ULTRIX 4.3 (MIPS)
 - Linux (INTEL)
 - Sun Solaris
 - different versions
- Configuration
Easy and user-friendly to handle (nearly no additional administration time).
- Support
Free during a valid support period.
- Updates
Each database is continuously checked and updated.
AUTEM provides periodical updates of the PERKEO®-Library during a valid update- and support-service
- Prices (product, support, updates,..)
Ask for quote at info@perkeo.net
- Extra, useful information about the product / Documentation
/

A.44. PureSight of iCognito

Unisys

NAME and version of the product:

PureSight PC (version 2.6) and PureSight (version 4.5)

Company (name and address):

iCognito Inc.

Address not specified on the website

URL Home site:

<http://www.icognito.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
ACR™ – Advanced Content Recognito -- Analysis of HTML

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
They do not classify the content into a database, the classification is made on-the-fly. The classification engine is based on a category profile that is developed by their Content Classification group under the management of a Library Information Specialist.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Escort Services, Erotic Stories, Fetish

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Any organization with Internet access and concerns about the content entering their network is targeted.

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Redirect to another site.

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Reports can be generated.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Over 90-99% in benchmarks.

14. Product description:

- Options
/
- Security
/
- Technical Requirements (Platform, type of browsers compliant with,...)
Compatible with all commonly used browsers
PureSight PC (Client Version):
Supports Windows 95/98/ME/2000/NT/XP
PureSight (Server Version):
Available for MS ISA, MS Proxy, Squid and Check Point FW-1
- Configuration
PureSight system architecture supports easy deployment of an Internet Acceptable Use policy in a high availability network. The policy can be centrally managed and deployed to an unlimited number of filtering enforcement points. Automatic distribution of configuration changes eliminates the need to configure servers independently and the solution easily scales as the network grows, simply by deploying additional PureSight content filtering servers.
The following modules form the total PureSight solution:
PureSight Content Filtering Server
PureSight Management Server
PureSight Log Server
- Support
Available direct from reseller or via email from iCognito: support@icognito.com
- Updates
Updates are handled automatically.
- Prices (product, support, updates,..)
Prices depend on configuration, number of users, etc.
- Extra, useful information about the product / Documentation
/

A.45. R3000 of 8e6 Technologies

NAME and version of the product:

R3000

Company (name and address):

8e6 Technologies

282 West Taft Avenue

Orange, CA 92865

URL Home site:

<http://www.8e6.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

Pass-by. Definition: Pass-by hardware solutions such as the R3000 are placed outside the flow of network traffic. It "watches" rather than "stops and checks" Web site requests. The result: no slowdown, even in heavy traffic situations. Most importantly, it doesn't create a point of failure.

2. What does the product control (the scope)?

- Access to web pages
 - Use of e-mail
 - Spam
 - Attachments of emails
 - Online chat rooms
 - Movement of files in and out of your computer (FTP)
 - Access to newsgroups (Usenet)
 - Access to various forms of instant messaging
 - E-commerce, credit card usage
 - Offline (non-Internet) computer use
 - Access to other Internet capabilities, please specify:
Peer-To-Peer
-

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
8e6 Staff

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Activity is logged

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

- YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input checked="" type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Other, please specify: Only the Sys Admin or 8e6 can make modifications, not the end user.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Above 99.4%

14. Product description:

- Options
Please refer to Account Exec, Dennis Buenaventura, dbuena@8e6.com
- Security
Linux OS 8.0 using OpenSSH 3.7
- Technical Requirements (Platform, type of browsers compliant with,...)
It works with any browser and any OS in any TCP/IP network.
- Configuration
Through GUI
- Support
24 hours tech support for critical issues.
- Updates
Nightly library updates of new URLs.
- Prices (product, support, updates,..)
Please check with Account Exec, Dennis Buenaventura, dbuena@8e6.com
- Extra, useful information about the product / Documentation
Please check with Account Exec, Dennis Buenaventura, dbuena@8e6.com

A.46. SentryCam

Unisys

NAME and version of the product:

SentryCam

Company (name and address):

Address not specified on the website.

URL Home site:

<http://www.sentrycam.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Monitoring software for parents

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
The software does not control but monitors all of the above.

3. Where can / must the product be situated?

- End user
 - Server or ISP
 - ISP and User
-

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Not applicable

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Key – capturing, ports tracing, etc

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
Not applicable | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not applicable

14. Product description:

- Options

Auto Monitor Comm Port for Activity when SentryCam Starts – This option tells SentryCam that when SentryCam starts, you want SentryCam to begin immediately watching the Comm port for any modem activity. NOTE: Since SentryCam does not know what function you may be using your modem for, that if you use your modem as a fax machine, it will begin taking screen shots while sending your fax.

Start taking screen shots automatically regardless of Modem Activity – This option tells SentryCam that you want to take screen shots from the moment SentryCam starts. This allows those on Cable or DSL Internet services to use SentryCam. Set this option if you use one of those services or if you want SentryCam to take screen shots of all activity on your computer.

Do not monitor Comm Port and do not start taking screen shots – This option tells SentryCam that you don't want to take screen shots when it starts and you don't want to monitor the Comm Port. This option is useful for temporary changes to your system and for faxing purposes. If you will be installing software, or faxing documents using your modem, you can select this option and when SentryCam boots backup again, it will ignore the Comm port and not take any shots unless you start it manually using the Start button on the main screen.

- Security

SentryCam can run in "stealth mode" meaning children are not aware that they are monitored by there parents. Configuration panel is only accessible with a valid user name / password.

- Technical Requirements (Platform, type of browsers compliant with,...)

Minimum Requirements :

Computer: Pentium 100 MHz or higher

Memory: 32 Mb RAM or higher

Operating System: Windows 95, 98, ME, (NT, 2000)

Recommended :

Computer: Pentium II 233 MHz or higher

Memory: 64 Mb RAM or higher

Operating System: Windows 98, ME

Optimum :

Computer: Pentium III, 500 MHz or higher

Memory: 128 Mb RAM or higher

Operating System: Windows 98, ME

- Configuration

Configuration is relatively easy and uses a wizard. Almost every feature is configurable.

- Support

Free email support and Online guide are available.

- Updates

Not specified on the website.

- Prices (product, support, updates,...)

34.95 \$ (US DOLLARS)

- Extra, useful information about the product / Documentation

/

A.47. SmartFilter of Secure Computing

Unisys

NAME and version of the product:

SmartFilter

Company (name and address):

Secure Computing

East Wing, Piper House

Hatch Lane

Windsor SL4 3QP

UNITED KINGDOM

Tel: +44.1753.410900

Fax: +44.1753.410910

URL Home site:

<http://www.securecomputing.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Violence, Drugs, Dating, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
 - Superior On-Box™ architecture
 - Accurate URL control list
 - Rich feature-set
 - Powerful reporting
- Security
 - Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Supported operating systems: Windows NT/2000/2003LinuxSolaris
 - Supported platforms available for download: Microsoft ISA Server
 - MS ISA Server SP1 for Windows 2000 SP2
 - MS ISA Server SP1 for Windows 2003 Microsoft Proxy Server
 - MS Proxy 2.0 SP1 for Windows NT SP6a (supported for SmartFilter 3.1.1 and earlier versions)
 - MS Proxy 2.0 SP1 for Windows 2000 Server SP2 (supported for SmartFilter 3.1.1 and earlier versions)
 - Sun ONE (iPlanet) Proxy Server
 - Sun ONE (iPlanet) 3.6 SP2 for Solaris 2.6 (UltraSPARC only), 8 Netscape Proxy ServerNetscape Proxy Server 3.5 SP2 for Solaris 2.6 (UltraSPARC only) (supported for SmartFilter 3.1.1 and earlier versions)
 - Squid Proxy ServerNOTE:
 - Check Point FireWall-1
 - Check Point FireWall-1 NG for Windows 2000 Server SP2
 - Check Point FireWall-1 NG for Solaris 8
 - SmartFilter® is also available on the following platforms:
 - Blue Coat Proxy SG
 - Cisco Content Engine and Content Engine Network ModuleComputer Associates eTrust Intrusion Detection
 - CrossBeam Systems
 - X40eSoft InstaGate
 - Hewlett Packard TRU64
 - Network Appliance NetCache
 - Ositis Win Proxy and eShieldSecure Computing Sidewinder® G2 Firewall™Vericept VIEW Filter
 - System requirements depend upon the environment into which SmartFilter® is being integrated, so please contact Secure Computing at 1.800.379.4944 or the local Secure Computing solution provider for the most up to date information.
- Configuration

Minimal administration :

SmartFilter's On-Box™ software plug-ins install in minutes and require no additional hardware or network changes.

Remotely manage multiple plug-ins on any mix of platforms right from the desktop.

Dynamic querying of user group information from external directories.

- Support

24x7 support

Live-answer support at no extra cost.

- Updates

All software and upgrades are included in the price: With SmartFilter, you benefit from an enterprise software license model. One has unrestricted access to the SmartFilter download site where one can download as many plug-ins as needed. If one has proxies running on different platforms? The paid subscription enables to download as many plug-ins, on as many platforms as needed, at no additional cost.

- Prices (product, support, updates,..)

The price is calculated per user.

- Extra, useful information about the product / Documentation

/

A.48. The SpamCop Email System of SpamCop

Unisys

NAME and version of the product:

The SpamCop Email System

Company (name and address):

SpamCop

Address not specified on the website.

URL Home site:

<http://www.spamcop.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:
Email filtering service

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
All mails are compared to SpamCop's own Spam mail servers

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
All sorts of spam

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
All spam mail gets blocked or put in a special map

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: Not specified on the website.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Email filtering
 - Email scanning
 - Spam reporting
- Security
 - Spam Cop also checks if mails contain viruses
- Technical Requirements (Platform, type of browsers compliant with,...)
 - The system works with PC's, Mac's, and any computer that can read standard internet email.
- Configuration
 - Very easy configuration online.
- Support
 - Online support is possible via administrated forums.
- Updates
 - No updates are necessary since all software is on Spamcop's side.
- Prices (product, support, updates,..)
 - The SpamCop Email System is priced at \$30 (US Dollars) per year.
- Extra, useful information about the product / Documentation
/

A.49. Surfcontrol Total Filtering Solution

Unisys

NAME and version of the product:
Surfcontrol Total Filtering Solution
Company (name and address):
SurfControl plc.
Riverside , Mountbatten Way
Congleton, Cheshire, CW12 1DY
UK
URL Home site:
<http://www.surfcontrol.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:
Popup and banner ad filtering

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Adaptative reasoning technology to control the flow of new websites in real time.
Language coverage : English, French, Dutch, Spanish, German

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

Over 40 categories exists. Every possible category is blockable. It's up to the administrator to choose which ones are ok.

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Corporate sector

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

Over 55 reports are generated: Top 10 HTTP, Top 10 FTP, Top 10 SMTP, Top 10 internet users, history of visited webpages, time log for individual users, etc.

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
 - Popup and banner ad filtering

- Bandwidth prioritization
- Time based activation of rules
- Multiple customizable deny pages
- Email notifications to managers in case of abuse
- Real/time monitor
- Comprehensive reporting
- etc.
- Security
 - Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Two versions are available :
 - 1. Platform Independent Version
 - ==> Linux, Windows 2000, Windows 2003
 - 2. Integrated platform solutions
 - ==> Microsoft Proxy Server, Microsoft ISA Server, Checkpoint Firewall, Novell Bordermanager, Nokia IPSO
- Configuration
 - Easy to use
 - Drag and drop rule creation
 - One click rule activation
 - Rule Sharing
 - Automatic Scheduling of reports
 - Automatic URL Category Database
- Support
 - Primary Level: Priority Maintenance Support
 - SurfControl's Primary Level of support includes access to the SurfControl dedicated Telephone Support Hotline and Priority E-mail Support, as well as free priority access to all version upgrades of your product during the term of your agreement.
 - Gold Level: Enhanced Personal Support*
 - SurfControl's Gold Level of support gives all of the Primary Level benefits with the added luxury and guidance of a dedicated TAM (Technical Account Manager) as your principal point of contact, as well as a back-up TAM in case of emergency.
 - * At this time, Gold and Platinum Levels are available in the U.S. and Canada only. Gold Level available to Primary Level contracts only.
 - Your SurfControl TAM will:
 - help you with your initial product training
 - assist you in developing a customized support plan to help drive the achievement of your key business goals
 - coordinate and streamline your support interactions
 - manage your incident escalation process
 - provide ongoing proactive services that identify common support issues
 - conduct periodic business reviews
 - Platinum Level: Vital Enterprise Support*
 - The Platinum level of support is designed to provide enterprise level professionals with the utmost in personalized service on the spot; it includes everything in the Gold and Primary Levels with the added assurance of Emergency Support 24 hours-a-day, 7 days-a-week, 365 days-a-year, for your mission critical issues. This is the level to have if you absolutely cannot afford the inconvenience and hassle of down-time.

- Updates
Updates are downloadable and free for minor modifications.
- Prices (product, support, updates,..)
For pricing info, please contact surfcontrol.
- Extra, useful information about the product / Documentation
A great number of case studies for several customers are present on the website:
http://www.surfcontrol.com/resources/Case_Studies/

A.50. The Bair of XEXOTROPE

Unisys

NAME and version of the product:

The Bair

Company (name and address):

XEXOTROPE

150 North Main Street

Elmira, NY 14901

Phone 607-767-0400

FAX 607-767-0481

URL Home site:

<http://www.thebair.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

For larger businesses, organizations, schools and libraries The BAIR recommends other BAIR services.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Artificial Intelligence tools

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

Bair stands for Basic Artificial Intelligence Routine – This sophisticated artificial intelligence program evaluates "on-the-fly," and it ensures that inappropriate text and images are filtered from view, yet it allows educational and informational content of a web site to appear.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
Violence, Drugs, Illegal, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Business

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify: Not specified on the website.	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
The BAIR PC software is Microsoft Windows 95, 98, NT, or 2000 compatible. Note that America Online (AOL) and Compuserve Internet connection services are not compatible with The BAIR Filtering System.
PCs configured for Networks (LANs) may not be compatible with The BAIR PC software.
- Configuration
Not specified on the website.
- Support
Not specified on the website.
- Updates
Not specified on the website.
- Prices (product, support, updates,..)
\$6.95 Monthly
- Extra, useful information about the product / Documentation
The initials B-A-I-R stand for Basic Artificial Intelligence Routine.

A.51. TOO COOL of Software 2010

Unisys

NAME and version of the product:

TOO COOL

Company (name and address):

Software 2010 LLC

2042 Corte del Nogal, Suite D

Carlsbad, CA 92009

United States

URL Home site:

<http://www.software2010.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Not specified on the website.

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not specified on the website.

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not specified on the website.

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|---|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
Not specified on the website. | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Software 2010 LLC uses industry standard security measures to protect against the loss, misuse and alteration of the information under our control.
- Technical Requirements (Platform, type of browsers compliant with,...)
The Software 2010 installation and programs on it are designated for use on Windows operating systems only and will not run on a Macintosh system. (WIN95/98/ME)
- Configuration
No configuration – just install and surf.
- Support
Free email and phone support – Online Faq.
- Updates
Updates are free of charge.
- Prices (product, support, updates,..)
\$5.00 USD monthly for the browser use.
- Extra, useful information about the product / Documentation
/

A.52. WatchDog

Unisys

NAME and version of the product:

WatchDog

Company (name and address):

Address not specified on the website.

URL Home site:

<http://www.sarna.net/watchdog/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

Watchdog is a monitoring program, it controls actions done by endusers on a PC. Watchdog can be installed on a single pc as well as on a network using a server.

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:
Not applicable

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:
Not applicable

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:
Not applicable

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not applicable

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
Key capturing

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|--------------------------|--------------------------|
| <input type="checkbox"/> The list of keywords | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The list of filtered URL's | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Other, please specify:
Not applicable | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not applicable

14. Product description:

- Options
 - Restrict:
 - Time Limits – Based on monthly, weekly, daily, one-time, or unlimited
 - Maximum time per login and minimum time between logins
 - Allow extra minutes on weekdays/weekends
 - Ability to carry-over unused time
 - Restrict the time of day the user can login
 - Program restrictions (file name) – Restrict how much time a user can spend in an application on a daily/weekly/monthly basis, and when they can run the application. Programs can be blocked by their file name or checksum so they are still tracked if renamed.
 - Program restrictions (window title) – Close windows that contain specific captions
 - Monitor:
 - Web pages visited in both Internet Explorer and Netscape
 - Keyboard typing in any application
 - Applications that were run (and when they started and stopped)
 - Screen shots of the session
- Security
 - Ability to run hidden from users
 - Single or multiple passwords per user
- Technical Requirements (Platform, type of browsers compliant with,...)
 - IBM PC or 100% compatible
 - 486/33 MHz processor
 - 4 MB RAM
 - 4 MB Hard Disk Space
 - Windows 95, 98, Me, NT (with SP5 or higher), 2000, XP, or 2003
 - Internet Explorer 5.05 or higher
 - TCP/IP network for networking

There are some Windows system components that WatchDog needs installed before it can run.

Required files:

All versions of Windows (95, 98, NT, 2000, XP, 2003): Internet Explorer 5.5 or higher

Windows 95, 98 and NT: Necessary to have the following Microsoft component installed: Active Directory Service Interfaces (ADSI) 2.5

Windows NT: Necessary to have the following Microsoft component installed: Active Directory Client Extensions (for NT4)
- Configuration
 - Profiles available to simplify management of users and save memory.
- Support
 - Free Email support, online guides and FAQ
- Updates
 - Not specified on the website.
- Prices (product, support, updates,..)
 - There are two packaging options. A download-only version (no CD media) is available for US \$35. You may also order a shipped CD media version for US \$40.
- Extra, useful information about the product / Documentation
 - /

A.53. WebDoubler of Maxum Development Corp.

Unisys

NAME and version of the product:

WebDoubler

Company (name and address):

Maxum Development Corp.

P.O. Box 315

Crystal Lake, IL 60039 , USA

URL Home site:

<http://www.maxum.com/WebDoubler/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d I t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

This is configurable.

7. Which type(s) of public ("buyers") is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
Accelerates Internet access for an entire workgroup or organization
Maximizes existing Internet bandwidth
Tracks Internet usage for usefulness and analysis
Controls use of Internet connection
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
WebDoubler requires a PowerPC Macintosh running Mac OS System 7.5 or higher and Open Transport 1.2 or higher. 680X0 Macs and MacTCP are not supported, due to the substantial performance requirements demanded by proxy-served Web traffic.
WebDoubler also requires at least 8 MB free RAM, and 12 MB or more is strongly recommended for improved cache effectiveness. Disk requirements are 5 MB for the WebDoubler installation, plus substantial space allocated for caching. Depending on the number of clients using WebDoubler, recommended disk space allocated for the WebDoubler cache can range from 100 Megabytes to several Gigabytes
- Configuration
WebDoubler requires an active Internet connection in order to serve external content to local users. In addition, local Internet users will require a TCP/IP connection to the WebDoubler Macintosh. The simplest WebDoubler configuration involves installing WebDoubler on a LAN where all clients have Web access through a single Internet connection using a router or gateway. In this case, WebDoubler can be installed on any Mac with Web access, and local client workstations can be configured to perform all Web requests through the WebDoubler proxy.
In addition, LANs can be configured so that only WebDoubler has direct Internet access. In this case, a single IP address is all that is required, and local client workstations will not be able to access Internet services without WebDoubler. Currently, this configuration is supported only when the WebDoubler Macintosh uses the same network adapter for both Internet access and client activity on the LAN. In the most common case, this means that clients on an Ethernet LAN cannot access the Web through a modem connection on the WebDoubler server. Instead, some routing solution must be added so that LAN activity and Internet connectivity is provided on the same network adapter, for example, and Ethernet connection.
- Support
User's Guides And Frequently Ask Questions (FAQs)
Mailing lists and Email support.
- Updates
At least 1 year of free upgrades.
- Prices (product, support, updates,..)

WebDoubler 1 CPU License	\$895.00
WebDoubler 3 CPU License (20% Discount)	\$2148.00
WebDoubler 5 CPU License (30% Discount)	\$3132.00
WebDoubler 10 CPU License (40% Discount)	\$5370.00

For all other situations request quote ==> <http://www.maxum.com/Sales/>
- Extra, useful information about the product / Documentation
/

A.54. We-Blocker

Unisys

NAME and version of the product:

We-Blocker

Company (name and address):

Address not specified on the website.

URL Home site:

<http://www.we-blocker.com/>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
violence, gambling, drugs and alcohol, hate speech, weaponry ,etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

8. Can the product be used without the knowledge of the person (child) being controlled?

Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the "places" listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

- | | REVIEW | MODIFY |
|--|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> The list of keywords | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> The list of filtered URL's | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> The company's criteria for inappropriateness a web page | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Other, please specify: | <input type="checkbox"/> | <input type="checkbox"/> |

13. What is the percentage of unwanted information correctly blocked?

Not specified on the website.

14. Product description:

- Options
/
- Security
Uses password protection that will prevent children from disabling or uninstalling We-Blocker.
- Technical Requirements (Platform, type of browsers compliant with,...)
200MHz Pentium processor
64 MB RAM
Windows 95/98/NT/ME/2000/XP
28.8 Modem
Internet connection
Internet Explorer 4 or newer
Netscape 3.02 or newer
5 MB of hard drive space
256 Color Display
- Configuration
Provides an Easy-wizard-like configuration ability.
- Support
FAQs and guides are provided for free.
There are three categories under which a technical support call will fall. The types of categories and the corresponding billing are listed below:
 1. Password Recovery
If you've lost your password and cannot remember your password the only alternative is to call tech support. A charge of \$10.00 will be made. We do not house your password at our facility. It is encrypted on your machine, and must be decrypted. This process will take approximately ten minutes, so allow for that time. You must be at the machine that has We-Blocker installed on it in order for password recovery to be possible. There is a fee of \$10.00 for password recovery.
 2. Manual Uninstall
If you or another user has deleted or changed files necessary for We-Blocker to run properly, we suggest you re-install We-Blocker to replace missing or damaged files. Should this prove unsuccessful, please call tech support for assistance. A manual uninstall requires approximately 15 to 30 minutes, so please allocate this time. There is a charge of \$20.00 for this procedure.
 3. General Issues
A general issue for which you need assistance is basically anything that could not be addressed via our FAQs or Tips and Tricks areas, and is not an issue that is determined to be due a system or program malfunction (i.e., user is responsible). Because the problem is not known beforehand and therefore, neither is the amount of time it will require, there is a \$20.00 charge for every 15 minutes that expire.
- Updates
Updates are provided for free.
- Prices (product, support, updates,..)
The product can be used free of charge.
- Extra, useful information about the product / Documentation
/

A.55. WebSense

NAME and version of the product:

WebSense

Company (name and address):

Websense Inc.

World Headquarters

10240 Sorrento Valley Rd

San Diego, California

92121

USA

URL Home site:

<http://www.websense.com>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) O t h e r , p l e a s e s p e c i f y :
violence, drugs, etc

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:
Businesses

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:
Not specified on the website.

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:
More than 80 reports can be generated on demand.
Real time traffic analyser: An interface for IT administrators that provides a real-time view of network activity within the last 24 hours.

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?
Not specified on the website.

14. Product description:

- Options
 - Detects malicious code, spyware , etc. on the system.
 - Blocks hacker intrusion
 - Manages bandwidth resources
 - Detects productivity problems
- Security
Not specified on the website.
- Technical Requirements (Platform, type of browsers compliant with,...)
 - Pentium III or greater processor with 512 MB RAM, or
 - Sun Ultra 10 Processor with 512 MB RAM.

WebSense supports Microsoft®Windows NT, Windows® 2000, Windows® 2003, Sun Solaris and Red Hat Linux operating systems.

For detailed technical requirements please check:
<http://www.websense.com/products/about/SysReqs/>
- Configuration
A user-friendly central management application manages all users and possible configurations.
- Support
Online Knowledge base, Guides and Faq is available.
Personal support has to be paid.
- Updates
Updates depend on the type of license.
- Prices (product, support, updates,..)
The price depends on solution requirements. On can request a quote via the website.
- Extra, useful information about the product / Documentation
/

A.56. WiseChoice Internet Filtering

NAME and version of the product:

Wisechoice Internet Filtering

Company (name and address):

2385 Vineville Ave. Suite 1, Macon, Ga.3120

URL Home site:

<http://www.wisechoice.net>

1. Product type:

- Special purpose browser for children
- Special search engine and portals
- ISP application
 - Conventional proxy application
 - Transparent proxy application
 - Specialized cache engine
- Restricted access application (e.g. by using age verification)
- Personal Computer application (Filter)
- Other, please specify:

2. What does the product control (the scope)?

- Access to web pages
- Use of e-mail
- Spam
- Attachments of emails
- Online chat rooms
- Movement of files in and out of your computer (FTP)
- Access to newsgroups (Usenet)
- Access to various forms of instant messaging
- E-commerce, credit card usage
- Offline (non-Internet) computer use
- Access to other Internet capabilities, please specify:

The filter gives 15 different categories of filtering which can be set up as a customized arrangement. The only default level of filtering is for pornography—other levels of filtering can be added at no extra charge—Three computers can be filtered per account. Up to five different filtering profiles may be set up per account allowing a filtering profile to be set up for adults, teenagers, small children etc according to their specific requirements.

3. Where can / must the product be situated?

- End user
- Server or ISP
- ISP and User

4. Which type(s) of technology does the product implement for control?

- Site labels or rating systems (PICS, an independent rating system)
- List of URLs
 - Black list
 - White list
- List of keywords
- List of keywords combined with analysis of the context in which they appear
- Analysis of image content
- Packet analysis
- Authorization
- Activity tracing
- Other, please specify:

5. By whom is the classification of the content done?

- Content providers
- Third-party experts
- Local administrators
- Survey or vote
- Automated tools
- Other, please specify:

6. What are the categories available to describe the different types of information controlled in the field of child pornography? These might include, for example,

- (a) N u d l t y (partial or full)
- (b) A d u l t p o r n o g r @ p h y
- (c) C h i l d p o r n o g r @ p h y
- (d) A n i m a l p o r n o g r @ p h y
- (e) G r o s s d e p i c t i o n s
- (f) S e x e d u c a t i o n
- (g) Other, please specify:

7. Which type(s) of public (“buyers”) is targeted?

- Parents
- Schools
- ISP
- Public points of access such as libraries,...
- Other, please specify:

Individuals including those with sexual addictions, also offices and small schools, churches etc.

8. Can the product be used without the knowledge of the person (child) being controlled?

- Yes / No

9. Set up and flexibility

- Online (downloadable)
- Offline (CD-Rom)
- Guided (Wizard) installation
- Non-guided installation
- The product can be adapted to predefined profiles

10. How is the person being controlled and warned when accessing inappropriate material?

- X-ing Out
- Page blocking
 - Simple message
 - Message with a full explanation of the reason
 - Configurable messages
- Other, please specify:

11. Does the product allow the user to trace the activities done in the “places” listed in question 2 (access to web page, e-mail, chat rooms, newsgroups,...)?

YES / NO

How is the information provided?

- Log / history files
- Screen capturing
- Capturing mouse-click
- Time logs
- Activities
- Other, please specify:

12. To what extent can the user act on the criteria for determining inappropriateness?

	REVIEW	MODIFY
<input type="checkbox"/> The list of keywords	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The list of filtered URL's	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The company's criteria for inappropriateness a web page	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify:	<input type="checkbox"/>	<input type="checkbox"/>

13. What is the percentage of unwanted information correctly blocked?

96%

14. Product description:

- Options
Up to five individualized filtering profiles per account–Up to three computers filtered per account.
- Security
The filter cannot be uninstalled by the end user without a live call to the office–attempts to delete the filter manually will result in no internet access.
- Technical Requirements (Platform, type of browsers compliant with,...)
Windows 95–XP
- Configuration
/
- Support
By telephone and email
- Updates
As needed
- Prices (product, support, updates,...)
\$5US per month
- Extra, useful information about the product / Documentation
This product is not an ISP. Wisechoice is downloaded and operates in conjunction with the existing service provider–it works with all ISPs except satellite access – It works also with DSL and cable access it cannot be turned off by the user. The office must be called to remove the filter by obtaining a password–attempts to erase the filter manually will result in no internet access.

APPENDIX 2: ILLUSTRATION OF A RATING SYSTEM, THE SAFESURF RATING STANDARD

From the official SafeSurf WebSite: <http://www.safesurf.com/ssplan.htm>

The SafeSurf SS~~ Rating Standard

Designed with input from thousands of parents and Net citizens to empower each family to make informed decisions concerning accessibility of online content.

Copyright 1995 SafeSurf Organization. All Rights Reserved.

Section One: Adult Themes with Caution Levels

SS~~000. Age Range

- 1) All Ages
- 2) Older Children
- 3) Teens
- 4) Older Teens
- 5) Adult Supervision Recommended
- 6) Adults
- 7) Limited to Adults
- 8) Adults Only
- 9) Explicitly for Adults

Section One: Adult Themes with Caution Levels

SS~~001. Profanity

- 1) Subtle Innuendo
Subtly Implied through the use of Slang
- 2) Explicit Innuendo
Explicitly implied through the use of Slang
- 3) Technical Reference
Dictionary, encyclopedic, news, technical references
- 4) Non-Graphic-Artistic
Limited non-sexual expletives used in a artistic fashion
- 5) Graphic-Artistic
Non-sexual expletives used in a artistic fashion
- 6) Graphic
Limited use of expletives and obscene gestures
- 7) Detailed Graphic
Casual use of expletives and obscene gestures.
- 8) Explicit Vulgarity
Heavy use of vulgar language and obscene gestures. Unsupervised Chat Rooms.
- 9) Explicit and Crude
Saturated with crude sexual references and gestures. Unsupervised Chat Rooms.

SS~~002. Heterosexual Themes

- 1) Subtle Innuendo
Subtly Implied through the use of metaphor

2) Explicit Innuendo

Explicitly implied (not described) through the use of metaphor

3) Technical Reference

Dictionary, encyclopedic, news, medical references

4) Non-Graphic-Artistic

Limited metaphoric descriptions used in an artistic fashion

5) Graphic-Artistic

Metaphoric descriptions used in an artistic fashion

6) Graphic

Descriptions of intimate sexual acts

7) Detailed Graphic

Descriptions of intimate details of sexual acts

8) Explicitly Graphic or Inviting Participation

Explicit Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

9) Explicit and Crude or Explicitly Inviting Participation

Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

SS~~003. Homosexual Themes

1) Subtle Innuendo

Subtly Implied through the use of metaphor

2) Explicit Innuendo

Explicitly implied (not described) through the use of metaphor

3) Technical Reference

Dictionary, encyclopedic, news, medical references

4) Non-Graphic-Artistic

Limited metaphoric descriptions used in an artistic fashion

5) Graphic-Artistic

Metaphoric descriptions used in an artistic fashion

6) Graphic

Descriptions of intimate sexual acts

7) Detailed Graphic

Descriptions of intimate details of sexual acts

8) Explicitly Graphic or Inviting Participation

Explicit descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

9) Explicit and Crude or Explicitly Inviting Participation

Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

SS~~004. Nudity

1) Subtle Innuendo

Subtly Implied through the use of composition, lighting, shaping, revealing clothing, etc.

2) Explicit Innuendo

Explicitly implied (not shown) through the use of composition, lighting, shaping or revealing clothing

3) Technical Reference

Dictionary, encyclopedic, news, medical references

4) Non-Graphic-Artistic

Classic works of art presented in public museums for family viewing

5) Graphic-Artistic

Artistically presented without full frontal nudity

6) Graphic

Artistically presented with frontal nudity

7) Detailed Graphic

Erotic frontal nudity

8) Explicit Vulgarly

Pornographic presentation, designed to appeal to prurient interests.

9) Explicit and Crude

Explicit pornographic presentation

SS~~005. Violence

1) Subtle Innuendo

2) Explicit Innuendo

3) Technical Reference

4) Non-Graphic-Artistic

5) Graphic-Artistic

6) Graphic

7) Detailed Graphic

8) Inviting Participation in Graphic Interactive Format

9) Encouraging Personal Participation, Weapon Making

SS~~006. Sex, Violence, and Profanity

1) Subtle Innuendo

2) Explicit Innuendo

3) Technical Reference

4) Non-Graphic-Artistic

5) Graphic-Artistic

6) Graphic

7) Detailed Graphic

8) Explicit Vulgarly

9) Explicit and Crude

SS~~007. Intolerance – (Intolerance of another person's racial, religious, or gender background)

1) Subtle Innuendo

2) Explicit Innuendo

3) Technical Reference

4) Non-Graphic-Literary

5) Graphic-Literary

6) Graphic Discussions

7) Endorsing Hatred

8) Endorsing Violent or Hateful Action

9) Advocating Violent or Hateful Action

SS~~008. Glorifying Drug Use

1) Subtle Innuendo

- 2) Explicit Innuendo
- 3) Technical Reference
- 4) Non-Graphic-Artistic
- 5) Graphic-Artistic
- 6) Graphic
- 7) Detailed Graphic
- 8) Simulated Interactive Participation
- 9) Soliciting Personal Participation

SS~~009. Other Adult Themes

- 1) Subtle Innuendo
- 2) Explicit Innuendo
- 3) Technical Reference
- 4) Non-Graphic-Artistic
- 5) Graphic-Artistic
- 6) Graphic
- 7) Detailed Graphic
- 8) Explicit Vulgarities
- 9) Explicit and Crude

SS~~00A. Gambling

- 1) Subtle Innuendo
- 2) Explicit Innuendo
- 3) Technical Discussion
- 4) Non-Graphic-Artistic, Advertising
- 5) Graphic-Artistic, Advertising
- 6) Simulated Gambling
- 7) Real Life Gambling without Stakes
- 8) Encouraging Interactive Real Life Participation with Stakes
- 9) Providing Means with Stakes