EG-S-NT (2002) 9 fin

The impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation

Final report of the Group of Specialists EG-S-NT

Directorate General of Human Rights
Strasbourg, 2003

Division Equality between Women and Men
Directorate General of Human Rights
Council of Europe
F-67075 Strasbourg Cedex

Imprimé dans les ateliers du Conseil de l'Europe

The Council of Europe

The Council of Europe is a political organisation which was founded on 5 May 1949 by ten European countries in order to promote greater unity between its members. It now numbers forty-five European states.[1]

The main aims of the organisation are to promote democracy, human rights and the rule of law, and to develop common responses to political, social, cultural and legal challenges in its member states. Since 1989 it has integrated most of the countries of central and eastern Europe and supported them in their efforts to implement and consolidate their political, legal and administrative reforms.

The Council of Europe has its permanent headquarters in Strasbourg (France). By Statute, it has two constituent organs: the Committee of Ministers, composed of the foreign ministers of the forty-five member states, and the Parliamentary Assembly, comprising delegations from the forty-five national parliaments. The Congress of Local and Regional Authorities of Europe represents the entities of local and regional self-government within the member states.

The European Court of Human Rights is the judicial body competent to adjudicate complaints brought against a state by individuals, associations or other contracting states on grounds of violation of the European Convention on Human Rights.

1. Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Georgia, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, "the former Yugoslav Republic of Macedonia", Turkey, Ukraine, United Kingdom.

The Council of Europe and equality between women and men

The consideration of equality between women and men, seen as a fundamental human right, is the responsibility of the Steering Committee for Equality between Women and Men (CDEG). The experts who form the Committee (one from each member state) are entrusted with the task of stimulating action at the national level, as well as within the Council of Europe, to achieve effective equality between women and men. To this end, the CDEG carries out analyses, studies and evaluations, defines strategies and political measures, and, where necessary, frames the appropriate legal instruments.

For further information on activities concerning equality between women and men, contact:

Division Equality between Women and Men
Directorate General of Human Rights
Council of Europe
F-67075 Strasbourg Cedex

Contents

“The fateful question for the human species seems to me to be whether and to what extent their cultural development will succeed in mastering the disturbance of their communal life by the human instinct of aggression and self-destruction.”

Sigmund Freud, 1929

Introduction

"Changing social mores and technologies are giving rise to new forms of delinquency."[1]

This observation dates from 1978. The boom in new technologies, in particular the Internet, has thus paved the way for new forms of crime, also known as cybercrime, including notably sexual exploitation and child pornography, and given a new dimension to the practice of trafficking in human beings for the purpose of sexual exploitation.

The Internet offers unprecedented advantages, which traffickers have been quick to exploit. The Internet and other types of telecommunication provide the sex industry and individual users with new ways of finding, marketing and delivering women and children into appalling conditions of sexual exploitation and modern-day slavery[2].

1. J. Carbonnier, *Sociologie juridique*, PUF, 1978, p. 401.
2. D. Hughes, "The impact of the use of new communications and information technologies on trafficking for the purpose of sexual exploitation in human beings for sexual exploitation."

The Council of Europe Summit of Heads of State and Government acknowledged the scale of the problem in 1997. Affirming its determination to combat violence against women and all forms of sexual exploitation of women, it called on the Council of Europe to develop a European policy for the application of new information technologies, with a view to ensuring respect for human rights and cultural diversity, fostering freedom of expression and information and maximising the educational and cultural potential of these technologies.

As part of this policy, the Council of Europe set up a Group of Specialists (EG-S-NT) to study the impact of new technologies on trafficking in human beings for the purpose of sexual exploitation. The group operated under the auspices of the Steering Committee for Equality between Women and Men (CDEG) and its work on this new aspect of trafficking in human beings for the purpose of sexual exploitation was a follow-up to the activities that have been pursued by the CDEG in this area since the early 1990s.

Terms of reference

Drawing on the work already done by the CDEG on trafficking in human beings for the purpose of sexual exploitation and by other national and international bodies, the group was instructed in particular to:

1. consider in depth the scale of the impact of the use of new information technologies on trafficking in human beings for purposes of sexual exploitation, specifying:
   - the techniques used and how they work;
   - the various kinds of users and their motives;
   - existing legislation in the member states and relevant international texts.
2. study the effects of the use of new technologies on the victims of trafficking for the purpose of sexual exploitation and the resulting violations of human rights, as well as the negative effects on some users;
3. prepare, on this basis, guidelines for media professionals, the boards of newspapers and other press and audiovisual media, public authorities and non-governmental organisations and associations, as well as any other persons involved.[3]

Composed of 8 experts in mass media, criminal law and gender equality appointed by the CDEG and other Council committees,[4] the Group of Specialists (EG-S-NT) began work in December 2000. It held five meetings between December 2000 and October 2002. This report is the result of their efforts.

It is a comprehensive report, based on the work undertaken by the Council of Europe and other international bodies in the area of trafficking in human beings for the purpose of sexual exploitation and supplemented by information and data gathered by the group on a subject that is still largely unexplored.

3. The terms of reference are set out in full in Appendix 1, p. 65.
4. See the list of experts in Appendix 2, p. 67.

Structure of the report

Together, these data determine the structure and scope of the report, which deals with three main issues:

I. The impact of the use of new information technologies on trafficking for the purpose of sexual exploitation in human beings and its scale: the techniques used and how they work, and the various kinds of users and their motives;
II. Existing legislation and its limits at national and international level and the role of the law in combating illegal or damaging use of the Internet;
III. The new challenges involved in protecting human rights and guaranteeing proper use of new technologies, in particular the effects of the use of new information technologies on the victims of trafficking for the purpose of sexual exploitation, freedom of expression and the Internet and the role of the media.

In order to perform its task, as well as incorporating the findings of work already done in this area, the group drew on the results of two studies which it commissioned from a consultant, Ms Donna Hughes, a researcher at the University of Rhode Island (USA). One looks at "the impact of the use of new communication and information technologies on trafficking in human beings for the purpose of sexual exploitation: a study of the users" and provides the framework for the first part of this report. The other examines the "role of marriage agencies in trafficking in women and trafficking in images for the purpose of sexual exploitation" in order to investigate the links between trafficking for the purpose of sexual exploitation and new information technologies, in particular the Internet.

These studies were supplemented by the findings of a questionnaire sent to all Council of Europe states, which covers factual information, users and victims, the legal framework, law enforcement and anti-trafficking for the purpose of sexual exploitation actions and cases, the mass media and prevention.

In addition, the group asked the Swiss Institute of Comparative Law to prepare a comparative study of the legislation in nine European countries for prosecuting persons involved in trafficking in children and adults on the Internet, for the purpose of sexual exploitation.

Before commencing work, members of the Group adopted a number of guidelines and agreed on certain definitions.

This being an issue that is often examined purely in the context of child pornography (as in the case of Interpol, for example), the Group decided to study the impact of new information technologies on trafficking in human beings for the purpose of sexual exploitation in the case of *both children and adults.*

It also decided to avoid stereotypes of any kind and to employ neutral terminology. It must not be assumed, for example, that the clients of the "sex industry" are mostly men and the use of new technologies in this context an exclusively male practice, or that women and children are always the victims. Hence the need to examine these issues closely in order to more clearly define the phenomena in question.

Definitions

Definition of "the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation"

As regards the definition of "the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation" in the context of the use of new technologies, the aim here was to widen the definition of trafficking in human beings for the purpose of sexual exploitation to include the virtual aspect, and to talk about virtual images which were detrimental to real people. There was a need to determine whether the concept of trafficking in human beings for the purpose of sexual exploitation necessarily involved physical movement, or whether attention should also be given to the case of people who did not actually leave the country, or the issue of virtual images. In order to do this, the Group referred to the definitions and most recent information contained in internationally approved instruments, namely

- the Convention of the United Nations on the Elimination of All Forms of Discrimination against Women (Article 6) and its monitoring system;
- the Protocol to Prevent, Suppress and Punish Trafficking for the purpose of sexual exploitation in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organised Crime, which was opened for signature on 14 December 2000;
- Recommendation No. R (2000) 11 adopted by the Committee of Ministers of the Council of Europe on 19 May 2000;
- the European Convention on Cybercrime adopted by the Committee of Ministers on 23 November 2001;
- Recommendation Rec (2001) 16 on the protection of children against sexual exploitation adopted by the Committee of Ministers on 31 October 2001 revising Committee of Ministers' Recommendation No. R (91) 11 concerning sexual exploitation, pornography and prostitution of, and trafficking for the purpose of sexual exploitation in, children and young adults.

The group noted, however, that neither the Council of Europe recommendations nor the European Convention on Cybercrime, nor the additional protocol to the UN Convention against Transnational Organised Crime, designed to prevent, suppress and punish trafficking in persons, especially women and children, covered the issue of virtual trafficking for the purpose of sexual exploitation.

It thus drew on the work of the Group of Specialists responsible for revising the recommendation concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults for the purpose of sexual exploitation, adopting its wider definition of trafficking for the purpose of sexual exploitation, which holds that "child pornography" does not necessarily imply the use of a "real" child and that broadcasting images or virtual images is sufficient to constitute child pornography as, even though there are no real children in-

volved, the victim is denoted by the image of the person thus depicted.

It was also felt that trafficking for the purpose of sexual exploitation should not be defined as in the UN protocol, purely as a transnational phenomenon, involving a crossing of borders, but could also be said to exist in cases where the victim did not physically leave the country and where images were transferred. Likewise, the UN convention addressed the problem solely in the context of organised crime. There was thus a need to widen the remit to include all the other instances of trafficking for the purpose of sexual exploitation.

The group also took the view that, especially in the context of human rights, trafficking in human beings for the purpose of sexual exploitation through the use of new information technologies was a comprehensive term encompassing child pornography, enforced prostitution and other forms of sexual exploitation.

Definition of new technologies

Not wishing to confine itself to the Internet, already regarded by some as "outdated", the group widened its study to include all the new media offering Internet-television-mobile-phone links.

Examples of how these technologies are used can be found in Ms Hughes' study, and more specifically in her study on "The role of Marriage Agencies in Trafficking in Women for the purpose of sexual exploitation and Trafficking in Images for the purpose of sexual exploitation".

As well as the problems involved in defining the various concepts featured in this report, the group was also required, under its terms of reference, to determine the scope, aims and objectives of the report. The problems and questions that arose in the course of this exercise are outlined below in the description of the different sections that make up the report. The idea was to show, through specific examples, the impact of new technologies on trafficking for the purpose of sexual exploitation, the current state of legislation in this area and the role that legislation could play in preventing the potentially harmful effect of new technologies and, above all, to show how human rights protection could be reconciled with guaranteeing proper use of new technologies.

The various contributions from the EG-S-NT specialists and outside consultants were used to produce findings and recommendations in each of the areas concerned, in the light of specific examples.

I. The impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation: the scale of the phenomenon

A. A study of the users

Ms Hughes, who prepared a study on this subject, focused her research on the use of new information technologies for trafficking in adult persons (over the age of 18) for the purpose of sexual exploitation (in particular recruitment of persons and exploitation of trafficked persons) and existing practices as regards images of adult persons (e.g. the case of people who do not physically leave the country but who are exploited sexually and whose images are then distributed without their consent on the Internet). To complement her work, reference was also made to the questionnaire replies.

The techniques used and how they work

In the light of the information gathered, the group has sought to emphasise the usefulness of new information technologies in general. At the same time, however, it is clear that these new technologies are being widely abused. Using the definition of new information technologies adopted by the group, various kinds of technologies can be used for the purpose of sexual exploitation – either by individuals for their own private use or by persons or groups using the Internet as a commercial tool, to promote and sell images or services.

The growth of these phenomena is also due to the inexpensive and accessible nature of new technologies (such as "web-cams", which can be used to broadcast all manner of images worldwide, at relatively little cost). These aspects are a key factor in making full use of the technical opportunities afforded by the Internet.

The various kinds of users and their motives

Who are the users? What are their motives? These questions had been singled out for research by the experts who drafted Committee of Ministers' Recommendation No. R (2000) 11,[1] as very little was known about these matters. In order to gather more information about Internet users and their motives, the Group carried out research in this area, based on the findings of Ms Hughes' work and existing studies in the field. It thus discovered that most users were involuntary users, often minors, in some cases lured into the business through harmful use of technologies by traffickers, and that these users were themselves potential victims.

1. Recommendation No. R (2000) 11 of the Committee of Ministers to member states on action against trafficking in human beings for the purpose of sexual exploitation, adopted by the Committee of Ministers on 19 May 2000.

B. Links between trafficking in human beings for the purpose of sexual exploitation and new information technologies and, in particular, the Internet

The additional study by Ms Hughes on the way new information technologies, and in particular the Internet, are used for trafficking for the purpose of sexual exploitation, both traditional and non-traditional (trafficking in images for the purpose of sexual exploitation) appears in this section of the report.

II. Existing legislation in the different member states and the relevant international instruments

The legal and legislative aspects are crucial for effective action against damaging use of new information technologies. The EG-S-NT thus decided to gather all available information on countries' legislation concerning the Internet and its unlawful and improper use.

A questionnaire on the legal framework, law enforcement and anti-trafficking for the purpose of sexual exploitation actions and cases, sent to all the member states, sought to determine the state of existing legislation and its limits at national level and the role of the law in combating illegal or damaging use of the Internet.

A. At national level

As regards the legal framework, it was clearly apparent that most member States had no legislation containing specific provisions regulating the use of new information technologies in order to combat trafficking in human beings for the purpose of sexual exploitation.

The group thus found that the laws currently in force in the various Council of Europe states made no attempt whatsoever to regulate the use of the Internet for trafficking in human beings for the purpose of sexual exploitation. Few countries dealt with each of the issues separately – namely the issue of content circulating on the Internet and the issue of trafficking in human beings for the purpose of sexual exploitation –, and, even when they did, no connection was made between the two.

It had hoped to carry out additional research on existing legislation at national level in order to compile a country-by-country inventory of laws on child and adult pornography, child and adult prostitution, on trafficking in human beings for the purpose of sexual exploitation in relation with new information technologies in order to form a clear picture of the limits of current legislation. This proved problematic, however, owing to the scale and complexity of the exercise.

The group accordingly asked the Swiss Institute of Comparative Law, which has some experience of dealing with harmful content on the Internet, to conduct a comparative study of the national legislation in nine member states for prosecuting persons involved in trafficking in children and adults for the purpose of sexual exploitation on the Internet. The following aspects of national legislation in relation with trafficking in human beings for the purpose of sexual exploitation were taken into account: the Internet (in particular, police powers to take action against unlawful sites), prostitution (in particular legal procedures for dealing with soliciting, procuring, etc.), pornography (in particular the age of consent), money laundering and the regulations on marriage agencies.

B. At international level

The main international legal instruments and the analytical reports dealing with trafficking in human beings for the purpose of sexual exploitation at international, regional and national level were pooled in order to highlight any aspects not covered at international level and a list of signatures and ratifications of the relevant international treaties drawn up.

The group was able to observe that there was no internationally approved instrument on the subject, i.e. the content circulating on the Internet in relation with trafficking in human beings for the purpose of sexual exploitation.

C. Combating illegal or harmful use of the Internet: role of the law

Legislation on the Internet is still very much in its infancy, and the difficulty of legislating in this area is compounded by the fact that the Web transcends national borders.

The group drew attention to the growing disparity between the attitude of the law towards child pornography, which is banned in a number of European countries, with access providers being forced to shut down certain websites, and its attitude towards trafficking in adult or mail-order brides for the purpose of sexual exploitation. In the case of these last two, the law is much less clear and legal action less effective. The group also noted an apparent decline in the number of prosecutions and decided to look into this, particularly in connection with the need to find ways of enforcing the said laws so that they were not simply ignored.

It also decided to gather and analyse details of relevant cases already settled which, even though the information they provided was often rather limited, could nevertheless be of use in studying the techniques employed and drawing broad conclusions. One notable example was the recent court case brought by the LICRA and the UEJF against Yahoo! and its French subsidiary.

III. Protecting human rights and guaranteeing the use of new technologies: new challenges

The use of new information technologies for trafficking in human beings for the purpose of sexual exploitation *creates different kinds of victims.* The Internet is used by traffickers to recruit potential victims although, in the course of its work, the Group identified other examples of victims as well.

The experts observed that that could lead to written and visual pornography becoming commonplace, and that the Internet could certainly be a factor in the current climate of growing tolerance towards documents and images of this kind.

Mention was also made of the links with *racism,* in that trafficking in human beings for the purpose of sexual exploitation is often related to immigration issues, but the group did not examine this question in depth as it was not part of its terms of reference. It noted however that the demand among users of

certain Internet sites for children and women of various ethnic origins is something that needs to be addressed.

A. Law enforcement and cases

The information was gleaned from the questionnaire replies, to which were added details of new cases, involving both children and adults, communicated by members of the Group.

As regards actions and cases, examples of action against trafficking in human beings for the purpose of sexual exploitation via new information technologies appear to be more common in the field of child pornography than in cases involving the exploitation of adult pornography or the exploitation of prostitution.

A fundamental knowledge of the development of this problem and its pro-active factors over the last decade could help to raise awareness (mistakes committed for empowering criminals, non-reactions, good practices of NGOs) and understand the whole complexity of the problem as well as the measures which should be taken.

B. The effects on the use of new information technologies on the victims – Protection of the victims

As regards protection, the focus is on victim's rights and the kind of assistance that is available to them (special therapy, etc.).

C. Prevention

The issue of prevention has been addressed in the light of information gleaned from the replies to the questionnaire. Particular attention has been given to the need to educate all the actors involved in the field of prevention.

The group also examined the way the illegal and harmful content on Internet could be fought.

D. The role of the mass media

The group decided to examine the role of the media in the light of the information gleaned from the questionnaire replies, and to include examples of good practice. In particular, it agreed that the matter needed to be considered in detail, as self-regulation of the media was a sensitive issue because of freedom of expression (the conflict of interest is particularly acute here because of financial factors: newspapers warn of the dangers of new technologies while carrying adverts for Internet sites and services).

The group also looked at how the media could play a key role in raising public awareness of these issues and contribute to prevention in general.

E. Freedom of expression and the Internet

The growth in crime and unlawful practices connected with Internet use is proof that public authorities cannot eschew all regulation in this area, in the name of freedom of expression. The question now is, what kind of legislation is needed to regulate the Internet, and what other forms of control are there, apart from laws and regulations? One option that has been suggested is to have codes of practice drawn up by Internet access providers themselves, for it would be very difficult to impose such codes on the media. The group also took into consideration the results of the Forum on harmful and illegal cyber content organised by the Council of Europe in November 2001 in Strasbourg.

Additional dossiers prepared on the basis of the replies to the questionnaire

- The legislative texts existing in certain countries (document EG-S-NT (2001) 6)
- Cases on the use of new information technologies in relation to child pornography, trafficking in human beings for the purpose of sexual exploitation as well as the dismantling of criminal networks (document EG-S-NT (2001) 7)
- Information on structures aiming to coordinate the fight against the harmful use of NCITs in relation to sexual exploitation and trafficking for the purpose of sexual exploitation in human beings (document EG-S-NT (2001) 8)
- Information on systems and good practices aimed at combating illegal or harmful actions perpetrated through NCITs (document EG-S-NT (2001) 9)
- Examples of preventive measures against the misuse of NCITs which have proved effective (document EG-S-NT (2001) 10).[1]

All these dossiers were used as inputs to this report.

The questionnaire was sent to the 43 member states of the Council of Europe: 31 replied. Answers were also received from two non-member countries (Monaco and Belarus) as well as from an international organisation (UNESCO).

In certain cases, several answers were received from the same country. This can be explained by the fact that several institutions with different qualifications were often consulted (police, migration services, bodies dealing with women's and children's

1. These documents can be consulted at the Council of Europe, Division of Equality between Women and Men.

rights, etc.). The different answers from the same country include complementary elements.

The answers to the questionnaire were provided by: specialised governmental bodies; police services; non-governmental organisations; departments or services within the following ministries: Interior, Foreign Affairs, Justice, Social and Family Affairs, Transport and Telecommunications; Offices of International Organisations, such as the IOM office in Hungary; UNESCO; representatives of the mass media. All these bodies work in the field of trafficking in human beings for the purpose of sexual exploitation from different perspectives.

I. The impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation: the scale of the phenomenon

This chapter is based on the results of the replies to the questionnaire sent to all the member states of the Council of Europe and of the studies made by Ms Hughes which describes how information technologies are used to facilitate the trafficking in human beings for the purpose of sexual exploitation and on the links between trafficking for the purpose of sexual exploitation and Internet.

On the basis of these results, it is important to underline the *usefulness* of Internet and of the new information technologies in general. The fact that Internet is a global network presents various advantages, including the possible use of the technology to better fight organised crime (as provided for by the United Nations Convention against Transnational Organized Crime opened for signature on 14 December 2000).

However, it is clear that the new technologies are largely *misused*. The growth of shadow economies and transnational criminal networks are negative manifestations of globalisation, arising from expanding economic, political and social transnational linkage which are increasingly beyond local and state control. Privatisation creates wider and more open marketplaces throughout the world, and the phenomenon is certainly boosted by a strong *demand* factor. Another important component of globalisation, computer communications technologies enable the increased volume and complexity of international financial transactions, which increase opportunities for transactional crime and decreased the probability of detention and apprehension. This technological aspect of globalisation enables the money gained through illegal activities to be transferred and laundered in any country.

The growth of these phenomena is also due to the inexpensive and accessible nature of new technologies (such as "webcams", which can be used to broadcast all manner of images worldwide, at relatively little cost). These aspects are a key factor in making full use of the technical opportunities afforded by the Internet.

Using the definition of new information technologies adopted by the group,[1] various kinds of technologies can be used for the purpose of sexual exploitation – either by individuals for their own private use or by persons or groups using the Internet as a commercial tool, to promote and sell images or services. Technical aspects are crucial for the developments of sites which exploit all the technical possibilities of the Internet. Often, the geographical location of the server (which can be situated in countries where the legislation in the field is weak or absent) neutralised the law. For example, even if some operations are prohibited by law in Europe (e.g. in Belgium), they are allowed by American legislation: it only takes a hyperlink from the Belgian site to an American one to neutralise the legislation.

The results of the studies commissioned from Ms Hughes and the findings of the questionnaire show that the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation is now seen as a serious issue.

Among the means used for communication and information, those seen as harmful or used in a harmful way, the most frequently mentioned in the replies to the questionnaire are the "Newsgroups", the World Wide Web pages and sites that convey information on where to find children/adults to be bought for sexual exploitation, Chat rooms or advertisements for the sexual exploitation or sex tours. In some answers, all the means mentioned in the questionnaire[2] are seen as being harmful. Even if for some countries this phenomenon is not yet widespread for the time being, in particular due to the relatively small number of computer users, the majority underlined the rapid increase in the use of NITs for the purpose of the exploitation of pornographic/sex related/trafficking in human beings topics over the last five years.

Among the main reasons given:

- The more and more generalised access to Internet.
- The number of users increases every year.

1. The group widened its study to include all the new media offering Internet-television-mobile-phone links.
2. The following means were listed: Newsgroups (and World Wide Web pages and sites) that convey information on where to find children/adults to be bought in prostitution; chat rooms; mail-order brides; live video conferences – transmission of live pornography or abuses of children and adults; advertisements for sexual exploitation of prostitution or sex tours.

- The price of the services is affordable.
- The users remain anonymous.
- The sale of pornography and other related material through Internet is a lucrative trade which does not require major investment.
- The lack of appropriate legislation or State policy to fight such a phenomenon.

Complementing these replies, the study made by Ms Hughes describes new information technologies, applications and services and how their features are used to facilitate the trafficking in women and children for the purpose of sexual exploitation. It is not an exhaustive list. All the types and uses are not categorised, but the most common and a few of the newest uses of these technologies of trafficking for the purpose of sexual exploitation of women and children are described.

Ms Hughes focuses on the use of new information technologies of trafficking in adult persons (over the age of 18) for the purpose of sexual exploitation (in particular recruitment of persons and exploitation of trafficked persons) and existing practices as regards images of adult persons (e.g. the case of people who do not physically leave the country but who are exploited by force sexually and whose images are then distributed on the Internet).

When doing her research, she noted that most of experts had only partial information. Although, they had expertise in one area, they knew nothing about another aspect. For example, someone may have knowledge of techniques used for computer crimes, but know little about trafficking in human beings for the purpose of sexual exploitation. The only people who had knowledge of both information technologies and trafficking in human beings for the purpose of sexual exploitation were those investigating child pornography or child stalking, but they knew little about trafficking for the purposes of prostitution or sexual exploitation of adults. *Consequently, a multidisciplinary approach is needed.*

Her research was based on the following sources in member States of the Council of Europe and the United States:

1. interviews with law enforcement officials
2. interviews with researchers on trafficking in human beings for the purpose of sexual exploitation, prostitution, pornography, and child sexual abuse
3. interviews with computer industry consultants
4. reports written by law enforcement personnel, researchers and NGOs
5. media news stories
6. content analysis of men's writings from the Internet about their sexual exploitation of women
7. unsolicited e-mail from men
8. original research on the Internet.

She described the new technologies, how they are used for the purpose of sexual exploitation, who are the users and finally the challenges society faces in confronting and ending trafficking in human beings for the purpose of sexual exploitation.

The results of her study are presented below.

A. A study of the users

1. The techniques used and how they work

New information technologies and services (the hardware), technology formats and information and computer applications (software) enable users to communicate and transmit files. None of these new technologies are in and of themselves harmful, but they provide those who wish to harm or exploit women and children with new, efficient and, often anonymous, ways of doing that.

New and old technologies

Established technologies such as television and cable being combined with new technologies to create new ways of delivering information, news, and entertainment. Web TV combines the television with the Internet. New cable networks use satellite transmission to deliver hundreds of channels and content on demand.

One does not usually think of mainstream communications, like cable TV, in connection with trafficking in women for the purpose of sexual exploitation, but images made using trafficked women may be transmitted to viewers through these venues. Satellite and cable companies say that the more sexually explicit the content the greater the demand. The explanation is that pornography on TV is increasing the total market by finding new buyers.

Although the Internet is becoming the primary way to transmit child pornography, the old-fashioned way of sending content – the mail – is still used by perpetrators, now in combination with Internet technology. The US Postal Inspection Service handles hundreds of cases of child pornography, and has found that increased use of the Internet by pedocriminals has increased their use of the US mail as well. The distribution of child pornography decreased from the early 1980s until five years ago. Then the Internet was invented. Since then the number of cases connected to the Internet has steadily increased. In 1998 32% of cases were Internet-connected. In 1999 the percent increased to 47%, and in 2000 77% were Internet-connected.[1]

Men in chat rooms trade small files – still images and short movie clips – on the Internet, but producers of child pornography advertise their videos on the Internet and distribute them through the mail. Stalkers talk to children in chat rooms, ask them to take pictures of themselves, and send them through the mail. When stalkers get children to travel to meet them, they send them bus and plane tickets through the mail.[2]

Scanners and video digitisers are used to turn old pornographic images, films and videos into electronic format that can be uploaded to the Internet. About half of the child pornography online is old images from films and magazines produced in the 1960s and 1970s.[3] Digital cameras and recorders enable the making of images that don't need to be professionally processed, thereby eliminating the risk of detection. These new types of equipment also make it technologically easier for

1. Interview, Raymond Smith, Fraud, Child exploitation and asset forfeiture group, Office of Criminal Investigations, US Postal Inspection Service, 7 May 2001.
2. Interview, Smith, 7 May 2001.
3. James F. McLaughlin, *Cyber Child Sex Offender Typology*, 2001.

people to become producers of pornography. Digital media formats are no longer static and independent. One format can be quickly converted into another. Videos are still the primary production medium for child pornography, and the still images for the Internet are produced by video capture.[1] From one video, 200–300 still images can be taken then uploaded to a newsgroup or Web site or traded one image at a time.

According to the COPINE (Combating Paedophile Information Networks in Europe) Project, production of child pornography still combines older methods of production, while using new Internet technologies for distribution.

> "At the moment the underground production of video child pornography may run parallel with, but be essentially unrelated to, Internet technologies for its distribution ... This may well change, however, as digital photography becomes more widely available."[2]

One police analysis noted that prior to the Internet the majority of collectors of child pornography did not distribute because duplication technology was not readily available. Now, making copies of image files "involves a few clicks of any computer mouse allowing for effortless distribution."[3]

Digital Video Disc (DVD) provides high quality videos and interactive capabilities for the viewer. While making the videos, scenes can be shot from multiple angles, and all points of view added to the CD-ROM. The viewer can then choose the version, point of view, or camera angle he/she prefers. Viewers can watch the movie in chronological order, moving from one character to the next, or watch the movie from one character's point of view. Viewers can interact with DVD movies in much the same way they do with video games, giving them a more active role.[4]

Although techniques like this have many applications and enable creativity and interactivity, it raises the question of the impact this has on people and their relationships and expectations of relationships. A portion of men who seek out women for the exploitation of prostitution do so because of their lack of social skills, or their misogynistic attitudes prevent them from establishing relationships with their peers. (See the later section on denial of the harm, p. 32.) Technology such as this may further distance some men from meaningful relationships.

Multimedia sex industries

Sex industries are embracing all technologies – old, new, and combined – to deliver their "adult content" to consumers.

In Europe, the two biggest sex industry companies have multiple media outlets for their products. A German company, Europe's largest pornography company, was listed on the Frankfurt stock market in 1999.

From Barcelona, Spain, another large sex industry company, which is listed on the NASDAQ, offers its content in a wide variety of media venues, but is increasingly moving into the high end Internet and satellite market.

These large companies are increasingly mainstreaming pornographic material. By their size, public listings on stock exchanges, and profit making, the sex industry has been legitimated.

1. Max Taylor, Ethel Quayle and Gemma Holland, *Child Pornography, the Internet and Offending*, 2000.
2. Taylor, Quayle and Holland, 2000.
3. McLaughlin, 2001.
4. Karen Kaplan, "Pushing porn on DVDs", *Los Angeles Times*, 9 January 2001.

Internet venues, applications and services

There are a number of venues and media formats with different technologies on the Internet for transfer of files and communications – Usenet newsgroups, World Wide Web, email, live synchronous communication (text and voice chat), bulletin or message boards, Web cams for live transmission of images or videos, live video conferencing (live video chat), streaming video, peer to peer servers, and file sharing programs. All forums and applications offer ways to engage in the sexual exploitation of women and children.

How each is used for sexual exploitation depends on the legality of the activity, which varies from country to country, the techniques adopted by the sex industry or individual users, and the level of privacy or secrecy attempted by the users.

Sex industries and perpetrators

The sex industry has aggressively adopted, and in a few cases, invented, every new communications and information technology for the marketing, selling and transmitting of pornographic materials and live sex shows. Perpetrators have also taken advantage of each new technology and application to stalk victims, transmit illegal materials, and avoid detection by law enforcement. According to one official, "If it can be done, they're doing it."[5]

❖ Newsgroups

Usenet newsgroups are still popular sites for the exchange of information about how to find women and children for the purpose of sexual exploitation. Although much media attention has been given to child pornography rings and cases that use sophisticated technologies and applications to keep their activities secret, the older public newsgroups are still commonly used to upload and download child pornography. According to one research source there are over 1000 illegal images posted on newsgroups each week.[6]

❖ Web message and bulletin boards

Web-based message boards and bulletin boards are increasingly popular for exchange of information by perpetrators of sexual exploitation. They are used in much the same way as newsgroups, but can be private and protected by passwords.

❖ Web sites

Web sites are the most popular venue for the distribution of pornography online. Large legal sex industry businesses have sophisticated sites with subscription fees that bring in millions of dollars per year. There are tens of thousands of free pornography sites that are maintained by amateurs or someone making a relatively small amount of money from advertising banners for larger sites and businesses.

Web sites can now offer streaming videos that can be viewed with Web browsers. The most recent versions of Web browsers come packaged with these plug-ins.

❖ Chat rooms

Real time synchronous communication or "chat" is a popular means of communication on the Internet. Chat is available

5. Interview, Glenn Nick, US Customs Cyber Smuggling Centre, 17 May 2001.
6. Taylor, Quayle and Holland, 2000.

through Internet Relay Chat (IRC) channels, Instant Messaging, such as ICQ, Web based chat sites which are accessed through browsers, Multi-User Dimension (MUD) or Multi-User Simulated or Share Hallucination (MUSH) programs. There are over 100000 chat rooms available to users worldwide. Some of these formats and the "rooms" they create are open to the public, some are private and require passwords, and others are used for one to one communication. No messages are archived or stored and no log files are maintained, as is done with e-mails or Web accesses, so stalkers use them to look for victims. There have been numerous cases in the US and UK of perpetrators contacting children for online and physical meetings in which children have been emotionally and sexually abused. There have been numerous cases of online stalking of adults that began with conversations in chat rooms, and led to physical meetings that turned into sexual assaults. One of the friendly features of ICQ that can have dangerous implications for children being stalked is the instant alert message that is sent out when one of the user's "buddies" logs on to the Internet.

❖ File transfer protocol

Although one of the oldest ways of exchanging files on the Internet, ftp (file transfer protocol), is still popular with pedocriminals for one-to-one exchange of child pornography. Ftp allows users to have direct access to another's computer hard drive to upload and download files. This technique of file exchange is most likely to occur between child pornography collectors who have met in other venues and come trust each other.

❖ Search engines

Even the everyday search engine can contribute to the expansion of sexual exploitation. Search engines are becoming more sophisticated and powerful in indexing the content of cyberspace. As a result users seeking particular types of pornography, women, children, locations, etc. can find it faster and with more precision. As a computer industry consultant said, "The discerning pornography users can find it faster. They no longer have to just stumble upon it."[1]

❖ Peer-to-peer networks and file-swapping programs

Recently, a new technology was developed and released as freeware that can create a network of peer computers. The result is an open, decentralised, peer-to-peer system. File-swapping programs are used to find files on the network. Using the program the user designates one directory on his/her computer that will be open to the public and another for downloaded files. When the user logs onto the Internet, he/she will be automatically connected to all other people running the same program. All available files are indexed into a large searchable database. When keywords are entered the request moves from one computer to the next returning links to files. Then the program can download the requested files from other member's network computers.[2] It is being toted as a revolution in how computers and people communicate with each other on the Internet.

These programs create a decentralised system, meaning there is no central server through which all communications pass. Consequently, there are no logs of transmissions, and transmissions are not traceable because each site can only trace the connection back one level. You can enter the public network or create a private one of your own.[3] These features are what make this new information technology so attractive to perpetrators.

Another program claims to take anonymity one step further by disguising the user as well.[4]

❖ Encryption

When criminal activity on the Internet is talked about, encryption is always mentioned as a technology likely to be adopted to disguise the content of files. Several law enforcement officials in UK and the US indicated that at this point the capabilities and threat of encryption seemed to be talked about more than it is used.

❖ Unethical practices

The sex industry has adopted many unethical practices to draw attention to their Web sites, and trap users once they are there. The sex industry advertises through banners on search engines, Web sites with free pornography, and spam – unsolicited e-mail. Almost everyone with an e-mail account has received unsolicited e-mail messages with advertising from the sex industry. "Click here for xxx." The goal of the "spammers" is to send millions of spam to accounts each day. They have no way of knowing who is receiving their messages. Children are as likely to get a pornographic spam as an adult. Spam costs Internet service providers millions of dollars by using their bandwidth, clogging their systems, and taking time to responding to angry customers. Even with aggressive efforts to block spam, a few spams consistently get through the traps.

The sex industry uses techniques such as "page-jacking" and "mouse-trapping" to pull in people who had no intention of visiting a pornographic Web site, then trapping them there as page after page of pornography opens up when the viewer tries to leave the site. Page jacking is a technique the sex industry uses to misdirect users so they mistakenly come to their Web sites. The include false key word descriptions or meta-tags on their Web pages so that search engines index the pages under those false descriptors. The users will then click on the link of their chosen topic, only to find themselves on a pornographic Web site.

Pornographers are very aggressive about using popular current events and search subjects to misdirect viewers.

Once intended or unintended viewers are on pornographic sites, the sex industry traps them on their pornographic sites using a technique known as "mouse-trapping." Sex industry Web page designers disable browser commands, such as "back" or "close," so that viewers cannot leave the site. When these buttons are clicked, another pornographic Web site opens up, resulting in endless numbers of pages opening on the viewer's screen. The sex industry has no idea who they are trapping on their Web sites, whether they are children or those who fervently do not want to view pornography.

1. Interview, Jeff Middleton, *Computer Focus*, USA, 17 May 2001.
2. "Gnutella – Welcome to Gnutella", site accessed 1 May 2001.
3. Ron Harris "Gnutella gives copyright holders headaches", Associated Press, 10 April 2000.
4. Berst, 24 April 2000.

❖ Anonymity and disguise

For those engaging in criminal activity anonymity, disguise or difficulty tracing their communication is critical. In an attempt to avoid being traced, criminals can send their communication through a series of carriers, each using different communications technologies, such as local telephone companies, long distance telephone companies, Internet service providers, wireless networks, and satellite networks. They can send the communication through a number of different countries in different time zones, where it is night in at least one place. This complicated routing makes the communication difficult to trace for technical, bureaucratic, political, and logistical reasons. In an attempt to avoid being identified, criminals can send their messages through a series of anonymous re-mailers who strip off identifying headers and replace them with new ones. One re-mailer service removed identifying features from the header, then held all incoming message until five minutes after the hour, then resent them in random order in order to make tracing an individual message more difficult. Messages could be sent through five to twenty other re-mailers with at least one located in a country known for its lack of co-operation with the global community and law enforcement.

Users of cellular and satellite phones can be located far from their home bases and still use their phones. Mobile phones can be programmed to transmit false identification. Also, criminals can sign up for mobile phone services, then throw the phone away after a short period of time or after a specific crime is committed. Pre-paid phone cards also can be used anonymously.

New technologies like Web TV, in which Web communications are displayed on a TV, don't have a file cache, like browsers installed on a computer. Therefore, no illegal material will be accidentally left in the cache to be discovered by police.[1]

❖ New technologies, new capacities, and increased production and distribution

New communications and information technologies have invigorated and enabled the trading, marketing and production of adult and child pornography. The new technologies have moved these activities into the home, where images can be scanned, produced, uploaded and downloaded in privacy. Even with the new production technologies, one of the earlier problems was storage space because of the size of the files, but now with zip and jazz drives, CDs and high capacity hard drives that isn't a problem. Perpetrators also use off-site or "cyberspace" storage, meaning they use other's computers clandestinely to store their files.

Transmission of files has become easier and there are more ways to disguise oneself. Improved Internet connections, such as cable modems, make is even faster. All of these technologies have made it easier to produce, store and distribute images of sexual exploitation.

1. Taylor, Quayle and Holland, 2000.

2. The use of new technologies

In the questionnaire sent to all member states, most of the persons contacted replied that, so far, no studies/research had been undertaken in their respective countries on persons using NITs with a pornographic/sex-related motivation. The exception seems to be Germany where a study was carried out in 1997 on child pornography by the Federal Office of Criminal Police in Wiesbaden;[2] the data from the European Centre for missing children "Child Focus" in Belgium should also be mentioned.[3]

No statistical information is available in the countries which have provided answers to the questionnaire. However, the answers mention some databases and general criminal statistics not related to the use of new technologies or also, in Switzerland, statistical data established by the police[4] and concerning the Internet from 1997 to 2000.

The research made by Ms Hughes describes how users and perpetrators use new communication and information technologies to traffic women and children for the purpose of sexual exploitation. This part is divided into sections according on how new technologies are used to carry out these activities. A few case examples from the United States and some European countries are provided.

All users want something different from the technology. Users seek different features from technologies. Criminals seek disguise and anonymity to knowingly commit crimes. Business and family men want privacy to engage in activities that may not be illegal, but considered immoral in their communities. Power users want speed, convenience and novelty. When the content or activity is for the purpose of sexual exploitation there is no consensus, no norms, and no homogenised laws to set a standard. What is legal in one country is illegal in another. Even laws that criminalise certain activities focus on different actions.

Communication among traffickers and pimps

There is little documentation of the use of new information technologies for criminal purposes by traffickers and pimps, but there is no reason to assume they are not using the latest technologies for their transnational or local activities. Pimps also use mobile phones for surveillance.

Criminals in general are using new communication technologies, such as mobile phones, to avoid police being able to trace phone calls. Mobile phone services often offer free or cheap phones for signing up for their services. Criminals use these phones for a weekend or a week, then throw them away. Pre-paid phone cards enable anonymous use of land line telephone systems. Trafficking in human beings for the purpose of sexual exploitation requires a lot of co-ordination – the recruiting, planning, travelling, meetings and transferring of people numerous times. It is likely they are using new technologies for ease of communication and to avoid detection.

In this case, the use of new technologies may not have increased the trafficking in human beings for the purpose of sexual exploitation, but it has made the activities easier. As more cases of trafficking for the purpose of sexual exploitation are uncovered, the details of their operations will mostly like reveal an increased use of electronic communications.

2. "Konzeption zu der Herstellung von und des Handels mit Kinderpornografie."
3. See document EG-S-NT (2001) 8.
4. Such as, for example, the number of complaints registered by the local police related to Article 197 of the Penal Code (hard pornography).

Traffickers and stalkers contacting victims

Traffickers and stalkers use the Internet in a number of ways to contact and recruit victims. There are many sites and forums on the Internet for adults to engage in sex talk, but child stalkers seek out children for the purpose of engaging in age-inappropriate graphic sex talk to provide sexual satisfaction for the perpetrator. Often the child stalkers will escalate by enticing the child to engage in more sexual activity, sometimes resulting in the perpetrator meeting the child. Perpetrators have also used various Internet forums to stalk adult victims. Crimes range from online harassment to physical stalking and sexual assault. Offenders have precipitated the victimisation of adults and children by third parties by posting messages, supposedly from the victims, asking for men to come and rape them or use them for the exploitation of prostitution.

❖ Traffickers recruiting victims

There seems to be some evidence that traffickers use the Internet to recruit women from sending regions to traffic them to western Europe. A report by the Denmark Police notes suspicious advertisements for nannies, waitresses and dancers on Web sites in Latvia and Lithuania.[1] The traffickers used Internet sites to post job advertisements for jobs in western Europe just as they do in magazines and newspapers. The magazine ads give mobile phone numbers for contacts, while the Internet sites give email addresses.

The significance of these Internet advertisements in the recruitment of women was disputed. Some thought that so few girls and women have Internet access in Latvia and Lithuania, especially in the poor, rural areas from which many girls/women are recruited, that this could not be an effective recruitment tool. Others thought that almost all girls or women would have access to the Internet through schools and libraries, where they may go to search for work abroad.[2] In Latvia, according to police sources, the women most vulnerable to recruitment were young women, aged 19 to 22, living in extreme poverty primarily in the southern and Russian part of Latvia where unemployment is high and the prospects for the future are poor. The destinations for the women from Latvia are primarily Germany and Scandinavia, but also include Great Britain, the Netherlands, Spain, Italy, Greece, Cyprus, Switzerland and Iceland. For the women from Lithuania, Poland is a transit country and Germany is considered to be the primary destination country, although many women are distributed to other European countries, especially Spain, the Netherlands, and Israel from there. Law enforcement sources believe there is a national network of recruiters in Lithuania with connections to international trafficking for the purpose of sexual exploitation networks.[3]

Stalking children in chat rooms

Stalkers use various forums on the Internet to contact, entice, and then assault and exploit victims of all ages.

There have been numerous cases of perpetrators stalking children online in chat rooms. There are nearly five million children using the Internet in the United Kingdom. Chat rooms are popular with teens, especially girls, who use it to communicate with their friends. In the UK, Internet users are perceived to be "clever, cool and trendy," rather than "geeks," a previous image. In the United Kingdom, the children that are at highest risk for "online enticement" by child stalkers are teenagers, mainly girls, between the ages of 13 and 17.

There are country and cultural differences in use of new information technologies. For example, in contrast to the United Kingdom trend where more girls use chat, in the United States and Canada, 60% of chat users are male.[4]

Children using chat are vulnerable to child stalkers who make contact with children online for various harmful purposes. Perpetrators engage children in age inappropriate sexual conversation or expose them to age inappropriate sexual material, including adult and child pornography. Perpetrators sexually exploit children online through sexual talk, making the children the subjects of their sexual fantasy. Perpetrators ask children to send them pictures or sexual images of themselves or their friends. They may encourage the children to perform sex acts on themselves or friends for the stalker's sexual satisfaction. Stalkers use these activities as part of a grooming process to entice children into more direct contact, such as telephone conversations and eventual physical meetings.[5]

When the child stalkers use voice chat they encourage the children to get headphones to reduce the risk of someone else in the house hearing the voices. They suggest that children get Web cameras for their computers and move their computers to their bedrooms where the man can encourage sexual acts while the man watches over a Web cam.

❖ Investigation of stalking in the United Kingdom

In one case in 2000 in England, a 33-year-old man met a 14-year-old girl in a chat room. He communicated with her through e-mail and mobile phone, then met her and raped her. He was arrested, but while on bail he was intercepted on his way to meet another 14-year-old girl he met in a chat room. He was convicted and sentenced to five years in prison. In another case in England, a 53-year-old man was convicted of sexual assault of a 13-year-old boy who contacted him through a gay counselling Web site. The man was sentenced to five years in prison.[6]

There has been at least one case of a British man travelling internationally to meet a child he contacted through a chat room. In 1999, a convicted paedophile from Newcastle was arrested when he flew to the United States to meet a 15 year-old girl. In May 2000, police in California discovered that a 28 year-old British man was trying to contact young girls in the US. Police from New Scotland Yard arrested him after their own investigation. [7]

The user of a mobile phone in the UK reported that the first text message she received asked her if she was a girl and how old she was. She thought this might indicate that stalkers are trawling mobile numbers to find girls.[8]

Last year, following the rape of a girl who was stalked online, ZDNet-UK investigated child stalker activity on Yahoo!'s chat rooms.[9] They found rooms with pedocriminal themes, such as

1. Denmark Police, report on the "Fact-finding mission" conducted in November 2000 by the National Commissioner of Police for the Baltic countries regarding trafficking in women, 2000.
2. Interview, Lisbet Jörgensen, Denmark Police, 2 May 2001.
3. Denmark Police, 2000.
4. Commerce Net, "Chat room use in North America", 30 August 2000.
5. Internet Crime Forum, March 2001.
6. Internet Crime Forum, March 2001.
7. Internet Crime Forum, March 2001.
8. Personal Communication, Balding, May 2001.

"11-16 gals for older men", "pics of preteen girls" and "naked babies to fuck".

ZDNet went into these chat rooms to document the chat room activities. They created a fictional 12-year-old, Tina Bell, who entered chat rooms and talked to others who found her there. Within seconds of entering a chat room "Tina" was solicited for sex with adult men. The men engaged in typical grooming techniques and ruses that child stalkers use to lure children into sexualised conversations and activities. After meeting the fictional "Tina" through chat, a man named Jim had her switch to voice chat using a microphone and Internet transmission. Jim engaged "Tina" in increasingly sexualised conversation over the next month, especially on the topic of having sex with adults.

Richard Berry, investigator for ZDNet, reported that several times advertising banners appeared with links to hardcore pornography. He wrote the following about his research into chat rooms on Yahoo!:

> "That work has revealed a predatory online culture where paedophiles are able to target children using sophisticated communications technologies, speak to them, form relationships with them and in some cases actually physically abuse them." [1]

The ZDNet-UK investigator condemned businesses and governments for their lack of accountability for the sexual abuse of children:

> "Abuse of children is being inadequately dealt with by a world leader in the New Economy.[2] Internet businesses refuse to be accountable in other countries, such as UK, even for endangerment of children, because they are based in the US and cite the United States Constitution's First Amendment as protection."[3]

❖ US girl stalked from Greece

Most cases of stalking are crimes committed by individuals that would not be considered trafficking for the purpose of sexual exploitation. Interestingly, some stalking and enticement cases show indications of being ways that traffickers recruit victims for the purpose of sexual exploitation.

A 37-year-old German man living in Greece contacted a 14-year-old girl from Florida in a chat room. He followed his Internet communication with letters by mail and telephone calls. After a year of corresponding, he convinced the girl to run away from home and come to Greece. To assist the girl in leaving home, he contacted a woman at a mobile phone store and convinced her to assist an "abused girl in leaving home." The woman met the 15-year-old, gave her a programmed cell phone and drove her to a local airport. The girl flew to Ohio, where another man, a convicted child pornographer, assisted the girl in getting a passport and leaving. The US Police were able to trace the travel and contacts of the girl by examining the email messages left on her computer at home.[4]

Upon investigation of the man who assisted the girl in Ohio, they found he to had pornographic images and videos of his 13- and 17-year-old daughters on his computer. He had been sexually abusing them for at least five years.

In Greece, the man kept the 15-year-old girl under control, locked in an apartment in Thessalonica. She was not permitted to answer the phone or the door. The girl's friends received e-mail messages sent from Internet cafés in Athens and Thessalonica saying that she was happy.[5] He told his mother that he felt pity for her because she suffered from leukaemia and he was trying to make her happy. He told the girl that he was a child psychologist who specialised in hypnotherapy and ran a youth centre.[6]

When he was found, he was charged with abduction of a minor with malicious intent, sexual assault and exposing a minor to improper material.[7] Investigation of his home found child pornography of other girls.[8] He is suspected of involvement with pornography rings on the Internet.[9] The girl suspects that he may have had other girls under his control and using them in making pornography. He was previously jailed on a fraud conviction.[10]

The international effort to find the missing girl involved the Polk County Sheriff's Office, US State Department, US Customs, US Postal Inspectors, the FBI, Interpol, US Embassy in Greece, the Greek Consulate and Greek police. The international cooperation has been praised, but also points out the effort needed to find one girl, and there are thousands of girls missing each year from parts of the world where such resources and cooperation do not exist.

Communication between pimps, pornographers and users

Men use e-mail, chat rooms, and Web sites to find pornographers selling child pornography and pimping children. There are reports of advertisements in newsgroups for children to be used in the production of child pornography.[11] On password protected bulletin boards people have offered or sought children for sexual abuse.[12]

❖ Distribution of Russian-produced child pornography; pimping Russian children

In February 2000, in a joint operation between Moscow City Police and US Customs agents, a man was arrested in Moscow for molesting children in the making of pornography. Four hundred tapes, 300 of them originals used for production, were seized. US Customs followed up on distribution of videos to the United States, resulting in five men being arrested. He made the pornography using boys who spent most of their time on the street in Moscow. The boys were easily recruited as a result of neglect or abuse by alcoholic parents. The tapes were marketed and distributed by an unemployed Russian stockbroker who

9. Richard Barry, "Chatroom danger – the making of the Tina Bell diaries", 15 March 2001.
1. Barry, 15 March 2001.
2. Barry, 15 March 2001.
3. Barry, 15 March 2001.
4. Interview, April Hindin, Postal Inspector, Tampa, Florida, 15 May 2001.
5. Jill King Greenwood "Missing girl case points to Greece, 2 suspects charged", *Tampa Tribune*, 27 January 2001, p. 12.
6. "Missing teen found, says she doesn't want to go home", *Athens News*, 2 February 2001.
7. "German man charged with luring Florida girl overseas", Associated Press, 3 February 2001.
8. "German man arrested", 3 February 2001.
9. "German suspected of links with pornography rings", *Athens News*, 6 February 2001.
10. "Missing teen found, says she doesn't want to go home", *Athens News*, 2 February 2001.
11. Eileen Gongora, "Pedophiles prey on children via Internet", *Star Banner*, 17 May 2001.
12. Toni Heinzl "Web site had 'child porn' link, detective testifies", *Fort Worth Star-Telegram*, 29 November 2000.

bought the tapes and resold them over the Internet. The tapes were delivered by mail.[1]

In addition to producing and distributing pornography, he acted as a pimp for child prostitution tourists coming to Moscow. Men from the US contacted him by email and had him make arrangements with the boys.

In another case in December 2000, Moscow City Police and US Customs uncovered a Web site operated by two Russians. They domestically trafficked children from Novokuybishevsk to Moscow (a distance of 560 miles) to be used in the production of child pornography.

In March 2001, Moscow City Police arrested a man known as the "Punisher" on charges that he sexually abused a 15-year-old boy in the making of two videos. The videos showed the rape and sadistic abuse of a boy who was visibly crying in the films.[2] Four hundred videotapes, video duplication equipment, and sales and shipping records were found. Buyers, who emailed the distributor their shipping address and wired cash for payment, were identified and arrested in Sweden, Denmark, the Netherlands and the US.

❖ Advertising trafficked women on the Web

Web pages have advertised trafficked women. Increasingly, the Web sites include photographs of the women, sometimes nude. This practice exposes women, identifying them to the public as prostitutes. Many of the photographs look like modelling photographs, and the women may never have intended those photographs to be used to advertise them as prostitutes. Some of the women may not even know their photographs are on Web sites. Women suffer from the stigma placed on them for being in prostitution. This public display and labelling further harms women in prostitution.

The only country for which there seems to a decline in Web advertisements for brothels and clubs is Sweden. The new Swedish law, which criminalises the buyers of women in prostitution, has deterred public advertising for prostitution. In a large public site for men to exchange information and reviews, there were only a few messages about prostitution in Sweden since 1999; all were warnings about the new law.

A Web search for Swedish "escorts," a popular euphemism for prostitute, found only a few sites. There are no explicit photographs, and of the few that were there, most did not show the women's faces. The few Web sites that advertise "escorts" give only a mobile number.

Communication among men seeking women and children for the purpose of sexual exploitation

Men seeking to buy women and children for the purpose of sexual exploitation and the making of pornography use forums on the Internet to exchange information about where to go and how much the women and children cost in cities all over Europe (and the rest of the world).

1. Interview, Marshal Heeger, US Assistant Customs Attaché, Moscow, Russia, 3 November 2000.
2. Terry Frieden, "Russia, US arrest suspects in global child porn ring" CNN, 26 March 2001.

❖ Latvian and Swedish child sex abusers and pornographers

Since the beginning of the 1990s men have been going to Latvia to sexually exploit women and children. In May 2000, as a result of co-operation of the Swedish and Latvian police, a Swedish citizen was detained on suspicion of sexually abusing Latvian children. His home was searched and Swedish police found a pornographic video of men sexually abusing two boys, ages 10-14. Swedish police identified two Swedish citizens and one Latvian citizen, and Latvian police identified others from the video. A Latvian citizen was charged with committing immoral acts with minors and inducing minors in the production of pornographic materials. Evidence collected in Latvia from the children in the film and the Latvian suspect was given to Swedish police, resulting in the successful prosecution of the Swedish man, as well. The Latvian and Swedish man had met and communicated their common interest in sexual abuse of boys and the making of child pornography over the Internet.[3]

❖ Communication about buying women and girls for the purpose of sexual exploitation

Men use the Usenet newsgroups to communicate with each other about where to go to find women and girls for sexual exploitation. To avoid detection, they use private chat rooms.

There are several public newsgroups and Web sites dedicated to finding and "reviewing" women and their performances. Women are referred to in misogynistic, obscene and degrading ways. A number of men describe coercing women to do what they want anyway.

Transmission of images, videos and live broadcasts

Every venue on the Internet is used to transmit images of sexual exploitation. The number of video clips is increasing and streaming video is available for those with high-speed Internet connections. Live Web broadcasts have become common. Almost all prosecution of the production and distribution of pornography has ceased so there are few cases to describe.

❖ Japanese women in live performances broadcast from US

In 2000, a case of smuggling/trafficking for the purpose of sexual exploitation was uncovered in Hawaii, USA in which Japanese women were brought into Honolulu to do live performances on the Internet for audiences in Japan.[4] Due to more restrictive laws concerning pornography in Japan, the men decided to operate their Web site from Hawaii and broadcast the live shows back to Japan. The Japanese men in Hawaii placed ads in Japan for "nude models." Upon their arrival in Hawaii, the women were used to make pornography and perform live Internet sex shows. The entire operation was aimed at a Japanese audience. The Web site was written in Japanese. The women performed strip shows by Web cam and responded to requests from men watching in Japan. They used wireless keyboards for live sex chat with the men at a rate of $1/minute. The Japanese men used digital cameras to capture the live video chat, then transmitted it to a server in California run by a "not respectable,

3. Personal communication, Pumpurs, May 2001.
4. "Immigration raid closes Internet porn site", Associated Press, 15 January 2000.

but not illegal" ISP. Japanese viewers accessed the performance through the California server.[1]

The defendants used e-mail to communicate between the smugglers and the women. They discussed how much money they would earn and where to wire the money. The Japanese men envisioned a much larger operation. They were planning on making pornography for Japanese buyers.

This case offers some twists in crime, smuggling/trafficking for the purpose of sexual exploitation and new technologies. James Chaparro, Director, Anti-Smuggling and Trafficking for the purpose of sexual exploitation Unit, US Immigration and Naturalization Service characterised the case in this way:

> "The Japanese men violated US immigration law by smuggling/trafficking for the purpose of sexual exploitation Japanese women into the US in order to circumvent the Japanese law against pornography."[2]

Omer Poirier, US Attorney in Honolulu, who handled the case described it this way:

> "Japanese men were smuggling women into the US from Japan to provide services for men in Japan."[3]

❖ Rape and torture images and videos

A Web site registered in Denmark claims it to have the "world's largest collection of real-life amateur slaves."[4] Men are encouraged to "submit a slave to the picture farm". Graphic descriptions of extremely violent acts are included in the advertisement.

A Web site registered in Moscow advertises itself as "the best and most violent rape site on earth". It claims to have "Several Hunders [sic] of rape pics". Subscribers are offered 30000 hardcore porn images, 500 online video channels, and 100 long, high quality videos.

Previously, few people had access to such extreme material. As one consultant explained,

> "Formerly men used to have to remove themselves from their community by three levels [to find extreme, violent pornography]. First, they had to go somewhere, physically, then know where to go, and then know how to find it. The Web makes it very easy to get that far removed very quickly."

❖ Sexual exploitation on the Internet

Trafficking for the purpose of sexual exploitation is a global organised crime. The resurgence of child pornography is a priority by law enforcement agencies, resulting in unparalleled international co-operation to break up the rings. In contrast, the production and distribution of pornography of adults and post adolescent teens has been completely ignored. In the US and Europe few, if any, cases against the producers or distributors of even the worst images are prosecuted.

A lot of the pornography is extremely misogynistic, with women portrayed as seeking and enjoying every type of humiliation, degradation, and painful sex act imaginable. Although, there is less information, it is likely that traffickers coerce women into making pornography[5] just as they coerce them into prostitution.

The availability of degrading, violent, misogynistic pornography is increasing, and the torture and bestiality images and videos are becoming more readily available. New technologies have enabled the average person with a computer, modem and search engine can find thousands of violent, degrading images within minutes that fifteen years ago they would never have found in a lifetime. The increase in video clips with audio and streaming video makes the action and harm come alive. New techniques, such as shockwave flash movies, enable the creation of animated videos. Skilled amateurs can create snuff films for distribution on the Web.

The Internet has made massive numbers and kinds of pornographic images easily available. In 1997, there were approximately 22000 Web sites with free pornographic content; by 2000 that number had risen to 280000.[6] In the United Kingdom there was a five-fold increase in child pornography from 215 cases in 1997 to 1128 in 1999.[7] In addition, the Internet lowers sexual inhibitions of users by normalising the images and behaviours, and providing a virtual support community for users online. Some users find that the risk of downloading illegal images adds to the excitement.[8] There is also evidence that images viewed on the Internet increase the amount of sexual activity. Offenders described trying to maintain a continuous state of arousal and masturbation the entire time they were online.[9]

The COPINE Project in Ireland in their analysis of collectors and producers of child pornography has decided that victimisation is the key place to start.

> "Each time a picture is accessed for sexual purposes it victimizes the individual concerned."[10]

In referring to a child pornography collection the researchers say,

> "In a sense, the function of picture collections for the offender is to repeatedly victimize the child concerned, and the victim status is exaggerated by continued use. ... an important purpose of child picture collections for the user is that it allows instant access to the child as victim."[11]

Although there are legal standards for child pornography, child pornography collectors have many images they collect for sexual purposes that do not meet the legal standard. Max Taylor of the COPINE Project realised the importance of analysing these images for their meaning to the offender, their place in his collection and his victimisation of children in the images.[12] The images can then be placed on a continuum of increased deliberate sexual victimisation. Through this type of analysis the researchers hope to arrive at an understanding of the factors that enable and sustain offender behaviour. This type of approach

1. Interview, Omer Poirier, US Attorney, Honolulu, Hawaii, 1 May 2001.
2. Interview, Chaparro, 1 May 2001.
3. Interview, Omer Poirier, US Attorney, Honolulu, Hawaii, 1 May 2001.
4. Interview, Jeff Middleton, *Computer Focus*, USA, 17 May 2001.
5. Liz Kelly and Dianne Butterworth, "Women's perspectives – pornography and the Internet", *Policing the Internet – Combating pornography and violence on the Internet – a European approach*, conference, London, UK, 13-14 February 1999.
6. "Questioning porn", *Los Angeles Times*, 19 May 2001.
7. Sara Gaines "Police are getting organised to catch crooks who thought the net offered a perfect forum", *The Guardian*, 26 April 2001.
8. Taylor, Quayle and Holland, 2000.
9. Taylor, Quayle and Holland, 2000.
10. Taylor, Quayle and Holland, 2000.
11. Taylor, Quayle and Holland, 2000.
12. Max Taylor "The nature and dimensions of child pornography on the Internet", *Combating child pornography on the Internet*, Vienna, 29 September-1 October 1999, http://www.stop-childpornog.at.

and analysis may reveal the goal of producers and users of pornography and the role it plays in creating and maintaining inequality between women and men.

Facilitation of access to pornography

One of the ongoing debates between the Internet industry, law enforcement and the public is how much responsibility service providers bear for the content on their servers or within their control.

❖ Internet service provider guilty of knowingly providing access to child pornography

In February 2001, in what was called a "groundbreaking case," an Internet service provider (ISP) in the US pleaded guilty to a charge of criminal facilitation for knowingly providing subscribers with access to child pornography through a newsgroup. Although the case was the first of its kind in the US, the New York State Attorney General said:

> "This case establishes a common sense standard for the Internet. When an ISP becomes aware of illegal child pornography available in its system, the ISP cannot put its head in the sand."[1]

The investigation was initiated two years ago, following the successful prosecution of members of a child pornography ring with members in US, Canada, Sweden and New Zealand. After dismantling the child pornography ring, the investigators turned their attention from the users of the newsgroup to the ISP that provided access to the newsgroup. This newsgroup published graphic images of child sexual abuse, and a 40-page-long FAQ (Frequently Asked Questions) on what the group was about, what images they could/should send and how to hide their identity, such as spoofing a header and using anonymous remailers.[2]

The ISP, in West Seneca, New York, took no action to remove the newsgroup after being notified by a customer and the police that child pornography was available there. The ISP also tried to quash almost a dozen subpoenas in the previous case. It refused to take action to remove the newsgroup even after police showed them graphic images, such as the rape of a four-year-old.

This case may set an important precedent for holding Internet service providers accountable for the material they knowingly transmit.

1. Press release "Breakthrough cited in war against child porn", 16 February 2001.
2. Interview, Paul McCarthy, Assistant Attorney General, Attorney General's Criminal Prosecutions Bureau, 21 May 2001.

3. The users

The collectors

Due to law enforcement actions against collectors, distributors and producers of child pornography, followed by analysis of the collections and collectors/distributors/producers, these perpetrators are beginning to be characterised to better understand their behaviours and the role information technologies play in trafficking in human beings for the purpose of sexual exploitation for the purpose of sexual exploitation.

At this time, the analysis of collectors has been limited to collectors of child pornography. It is known that some people have large collections of adult pornography. The specifics of the volume of their collections has sometime become public after their collections were discovered on work computers. Probably, many of the distributors of pornography on the Internet started off as collectors, then decided to make money from their collections.

❖ Collectors of child pornography and the role of the Internet

Through the analysis of its database of child pornography, the COPINE Project found that the majority of children used in the making of pornography are white, with fewer being Asian, and almost none being black. The analysis of images on child pornography newsgroups indicates that the average age of the children, especially the girls, is getting younger, and more images are being made of children from eastern Europe.[3]

The COPINE Project conducted interviews with those who downloaded and/or distributed and/or produced child pornography, and/or sexually assaulted a child. They found that people who use the Internet to download pornography are progressive in their offending behaviour that is directly related to their level of use of the Internet.

Offenders are people who have had early sexual behaviour (probably sexually abused themselves), have poor adult social skills, and are dissatisfied with their present selves. Acquiring a computer and computer skills enables them to enter a world where they can get satisfaction from images and fantasy and meet a virtual community of people who reinforce their behaviour. They may develop a sense of confidence in themselves for their new computer skills and success at building a large collection. Often, their collections took up more and more of their time as they sorted and catalogued the images they downloaded and traded.[4]

Most start out accessing adult pornography, then move on to child pornography. They continually move up to more sophisticated technologies and more extreme forms of sexual exploitation of children, either in seeking more harmful, extreme images, or the physical sexual abuse of children.

Collecting is an important psychological process and is directly connected to acquiring new technological skills. The offender becomes increasingly "empowered" by the combination of a physical collection, sexual satisfaction, computer skills and a supportive online community.

> "The rapid acquisition of images largely goes hand-in-hand with the acquisition of technical skills. Collecting also leads to an increase in fantasy and sexual activity, particularly masturbation in relation to images or through engaging in mutual fantasies with others while online. With increasing mastery of the Internet comes a sense of power and control."[5]

The COPINE Project found that those who collect child pornography through the Internet have many similarities with other child sex offenders. In addition, they had varying degrees

3. Taylor, Quayle and Holland, 2000.
4. Taylor, Quayle and Holland, 2000.
5. Taylor, Quayle and Holland, 2000.

of "function addition," resulting in mood modification, tolerance, withdrawal symptoms, conflict and relapse."[1]

Collectors of male child pornography

During a three-year Internet law-enforcement project conducted by the Keene Police Department, New Hampshire, USA, which focused on the sexual abuse of boys, 200 offenders were arrested. Of the 200 offenders, 143 were "collectors" of child pornography of boys. They ranged in age from 13 to 65 years old. Collectors and distributors, one as young as 14 years old, operated trading centres from their computers. The size of the collections ranged from a few hundred images to tens of thousands (on man had 43000 image files).

Collectors needed large computer storage, such as extra hard drives, zip and jazz disks, and CD-ROMS, to store all their images and videos. Some collectors used other people's computers, such as the high-school teacher arrested in Indiana, USA who had his collection on the high-school mainframe computer.[2] Others stored their collections in cyberspace, meaning they have access, either legally or illegally, to storage on servers or even private computers and connect to them through the Internet.

The Keene Police Department considered the collectors to be entry-level offenders. Most of them had no prior contact with law enforcement, and were not known to have sexually abused a child. The majority of the collectors were single, lived alone and socially isolated. Twenty-one percent of them were in occupations or vocations that brought them into contact with children.[3]

Many of the collectors started off collecting still images of children from newsgroups and Web pages that did not involve online interaction with others. Some then escalated to interacting with others in chat rooms. They also moved from collecting still images to video clips. Following that, some started to distribute child pornography. When the collectors interacted with other collectors they use their collections as currency to trade with other collectors, thereby moving from collectors to distributors.

Collectors become deeply involved with their collections, spending enormous amounts of time memorising hundreds, even thousands, of images, file names, and photographic series. They know if they have seen an image before and if it was renamed.

> "Massive child pornography collections with as many as 40,000 image files have been seized. These image files are divided and subdivided many times into folders according to age, hair colour, sex acts portrayed and many other categories. ... The amount of time it takes to download one picture, view it and place it in a file folder, multiplied by the size of the collection demonstrates the large investment of time these behaviours represent."[4]

Many of the child pornography collectors would never have engaged in this activity, certainly not to the extent they did, if not for the new information technologies that were available to them. The technology did not cause their interest or activity, but it played a heavy role in facilitating it.

1. Taylor, Quayle and Holland, 2000.
2. McLaughlin, 2001.
3. McLaughlin, 2001.
4. James M. McLaughlin, "Technophilia: a modern day paraphilia", *Knight stick: publication of the New Hampshire Police Association*, Spring/Summer 1998, Vol. 51, 47-51.

The stalkers

The Internet has become a favoured site for stalking children. Sex offenders can engage children on many levels, from sexual talk to enticing them into physical meeting. The many ways of disguising a person's identity have allowed many child sex stalkers to commit sex crimes against children with impunity. In 1995, an organisation that defends paedophilia as a type of "love" for boys, published an article which gave details on how to use the Internet to contact children.[5]

Online stalkers may themselves be adolescents. In 1998, Home Office, UK research found that adolescent sex offenders accounted for one third of all sex crime in the United Kingdom.[6] And a recent study by the National Centre for Missing and Exploited Children in the United States found that half of online solicitations involved juvenile offenders. It should be noted that these juvenile stalkers are themselves most likely previously or presently being sexually abused.

During a three-year Internet law-enforcement project conducted by the Keene Police Department, New Hampshire, USA, 200 offenders were arrested who targeted male children. (In this project, police officers entered chat rooms and newsgroups pretending to be boys.) Forty-eight of those men were "travellers", meaning they stalked boys online and eventually travelled to meet them. They ranged in age from 17 to 56, with a mean age of 35, and the following age distribution: 17 to29 (38%), 30s (25%), 40s (27%), and 50s (10%). Most, but not all, of these stalkers collected child pornography. Four of the men travelled internationally from Canada, Netherlands and Norway, and the others travelled from 10 different states in the United States. A few of the stalkers sent money, bus or airline tickets for the boys to use to run away and meet them.

Over half of the 48 men originally told boys that they were in their teens, then later revealed that they were older, although none gave their real (older) age. Over half of the 48 sent photographs, often naked, of themselves. The online conversations were aimed at building trust, engaging in sexual talk and sending pornographic images.

On one stalker's computer police found 25 transcripts of chats he had with boys from age 12 to 15 in five different states. He had convinced the boys to give him their names, addresses, directions to their homes, and cover stories to protect him.

The stalking of children on the Internet is receiving increasing attention and action from governments and law enforcement, but a member of the Keene Police Department, New Hampshire, USA believes that less than one percent of those committing crimes on the Internet are being apprehended.[7]

The buyers

Men who buy women and children for the purpose of sexual exploitation post information about their experiences in newsgroups and on the Web. They often reveal a lot about themselves: who they are, their attitudes toward women, and how they treat women.

Within the men's descriptions of their buying experiences are many hints of their use of trafficked women.

The men who use the Internet to find women trafficked for the purpose of sexual exploitation (and then write about their

5. McLaughlin, Spring/Summer 2001.
6. Internet Crime Forum, March 2001.
7. McLaughlin, 2001.

experiences there) seem to be mostly travelling businessmen, local men reporting on local prostitution, or students. Some of them say they consult newsgroups or Web sites before they travel and even print out the information to take with them. Some of the men write about their experiences buying women for the purpose of sexual exploitation as a way of reliving the experience. Some men include a lot of graphic details that indicate they are getting enjoyment out of reliving the experience through writing about it.

The producers

❖ Producers of child pornography

Most child pornography on the Internet is United States generated. According to Bruce Taylor, who formerly worked at the US Department of Justice's Child Exploitation and Obscenity Unit, now Director of the National Law Center for Children and Families:

> "The United States have more men on the Internet and more men making and using child pornography. We are still the leaders."[1]

During a three-year Internet law-enforcement project conducted by the Keene Police Department, New Hampshire, USA, 200 offenders were arrested who targeted male children. Of the 200 offenders they arrested, eight were producers of child pornography. They found that not all collectors of child pornography are producers but all producers are collectors. These eight offenders ranged in age from 26 to 53 with an average age of 41.

Sex offenders sent digital cameras to their contacts they thought were boys for them to connect them to their computers and send live sex acts to the men. The men planned to use video capture equipment to record the images and movies for later distribution. Offenders were also involved in secretly photographing children in public places or while asleep. They used hidden cameras in public bathrooms to capture images of children. Many of the offenders were still distributing images of children they had sexually abused years ago.

Most of the producers of child pornography were actively sexually abusing children or had criminal histories of sex offences with children. In four of the producer cases, runaway children were found in the homes of the offenders. The men engaged in many fetishes and paraphilias, as well. Only one man had made any money from the sale of child pornography over the Internet, and that was under US$1000.

The producers of child pornography were also more likely to be involved in other criminal activity. Police searches found offenders to have committed other crimes, such as: homicide, possession of explosives, controlled substance distribution and possession, firearms violations and the harbouring of runaways.[2]

Eastern European countries, particularly Russia, have become centres for the production of child pornography. "In many parts of Eastern Europe and Russia, 'anything goes,' as long as you pay a share of your profits to the 'mafia'." Another factor making eastern Europe a popular site for the production of child pornography is that the Slavic children are popular among collectors who prefer white children.[3]

In Budapest, Hungary, now known as the pornography production capital of Europe, there have been reports of young children – usually homeless or neglected – being recruited for pornography with promises of glamorous careers in modelling. In the town of Eger in northern Hungary, a man was arrested in June 1996 for using girls between the ages of 10 and 15 in his pornographic videos. He faced charges not for making the films, but for appearing in them. Under Hungarian law, children over the age of 14 can give "partial consent". This means a pornographic video produced with two 15-year-olds is not illegal, but a video of an adult having sex with a 15-year-old is. Moreover, in 1996, Hungary had no laws against the possession or distribution of child pornography. This lack of legislation provided child pornographers with attractive legal loopholes.[4] Things have changed now, as Hungary has adopted laws and regulations in this matter.[5]

Producers of adult pornography

Almost all sex industry companies are moving into new media venues, such as preparing for Internet broadband, and interactive hotel-room TV.[6] Adult pornography production is moving from the control of organised crime groups to big business in the United States and Europe. For several years, there has been a push on all fronts internationally to normalise and legitimise prostitution and pornography.

The United States is the largest pornography producer in the world. In California, where most of the production facilities are located, the pornography industry claims to employ 20000 people, and pay US$31 million in state sales tax on video sales alone.[7] In 2000 there were 11000 pornographic videos produced in the United States.[8] The online sex industry generated US$1.8 billion in revenue in 2000.[9]

Beyond the big money numbers, statistics on availability and demand for pornography on the Internet are becoming harder to find. Previously, there were statistics on the proportions of Web searches that were for pornography, the proportion of advertising revenue that came from the sex sites, etc. In the last year or two those statistics have disappeared. When Ms Hughes called the ratings and Internet research companies she was told that they no longer separated out statistics by "adult entertainment", at least those they are making available to the public. The "adult entertainment" numbers are now included in the "entertainment" or "advertisement" statistics. She believes that publishing statistics relating to the online sex industry was causing negative publicity for the Internet industries and the large corporations who have a stake in the sex and Internet industries. Therefore, a decision was made to no longer collect information specific to searches for pornography, etc., or not make it public. There were a few marketing reports for the online sex industry businesses, including for European markets.

1. Interview, Bruce Taylor, Director, National Law Center for Children and Families, 16 May 2001.
2. McLaughlin, 2001.
3. "Epicentre of child porn – Eastern Europe and Russia", site accessed 25 February 2001.
4. James Geary, "Sex, Lies and Budapest – as producers of sex films flock there, Hungary's capital is becoming Europe's porn capital as well", *Time*, 24 March 1997, Vol 149, No. 12.
5. See Chapter II of the report, "Existing legislation in the different member states and the relevant international instruments", p. 34.
6. F. Rich, 20 May 2001.
7. "Questioning porn", 19 May 2001.
8. Frank Rich, "Naked capitalists – there's no business like porn business", *New York Times*, 20 May 2001.
9. *Datamonitor*, UK.

Just because adult pornography is generating billions of dollars and big businesses have entered the market does not mean that the production standards of pornography have changed, especially for the women used in the videos. According to one producer:

> "Anyone with a video camera can be a director – there are countless bottom feeders selling nasty loops on used tape. Whatever the quality or origin of a product, it can at the very least be exhibited on one of the 70000 adult pay Web sites, about a quarter of which are owned by a few privately held companies that slice and dice the same content under different brands."[1]

As a result of the huge market on the Web for pornography and the competition among sites, the Internet images have become even rougher, more violent and degrading. One producer claimed that there were "no coerced" performances in pornography videos, although she immediately acknowledged that

> "there are little pipsqueaks who get their disgusting little videos out there. There's a trend in misogynistic porn, and it's upsetting."[2]

She went on to say,

> "I've been in the business for more than 20 years, and I helped make it possible for these guys to make these kinds of movies"[3]

Budapest – Pornography production capital

Budapest has become of one of Europe's pornography production capitals.[4] American and European pornography producers have moved to Budapest, Hungary because of the cheap, available actors from eastern and central Europe. Budapest provides low production costs, lax government regulations and attitudes, and beautiful scenery. There are hundreds of pornography films produced each year in Budapest. In only eight years, Budapest has become probably the biggest centre for pornography production in Europe, eclipsing rivals such as Amsterdam and Copenhagen.[5] A Hungarian film-maker produced the first all-Hungarian pornographic video. Between 1992 and 1997 he directed more than 30 feature-length pornographic films.[6]

The production of pornography in Budapest is looked upon as part of its new free market economy. A former Deputy Minister of Culture said, "Pornography is an industry for Hungary, not a tragedy."[7]

Pornography producers have been given unprecedented access to public and official sites to make their videos. The first American pornography director to film in Budapest directed a movie including a scene that was filmed on the city's busiest tram in the middle of the day. The tram travelled its normal route through a residential area, pausing at regular stops where people waiting for the tram witnessed the production. He claimed he was able to do this by bribing the streetcar controller with US$100 and a box of chocolates.[8] An Italian pornography producer has filmed ten movies in Budapest. One of his latest videos was produced in the library of a government ministry.[9] In 2000, the Minister of Education ordered an investigation after a German hard-core pornography producer used a prestigious high-school for its main set.[10]

Most west European producers of sex videos use east European actors wherever possible. "They cost less and do more," an executive at a German production company explains, bluntly.[11]

Budapest is a destination and transit city for women trafficked from Ukraine, Moldova, Russia, Romania, and Yugoslavia. In Budapest, the women are trained for enforced prostitution and issued fake documents before being sent to countries in western Europe.[12]

In 2000 police uncovered a trafficking for the purpose of sexual exploitation ring in Zuglo District of Budapest. An Austrian citizen organised a large trafficking enforced prostitution ring. The women were recruited from Kiev, Bucharest and Belgrade through advertisements in newspapers offering work as dancers in the West. When the women arrived in Budapest they were forced into prostitution and sent to Austria, Germany and Belgium. The network had branches in Ukraine, Serbia and Romania with people assigned to specific tasks, such as organiser, guard, driver, and drug-dealer. During a period of several months 300 women were trafficked through Budapest.[13]

Although the trafficking of women for the purpose of sexual exploitation into and through Budapest is widely recognised as a serious problem controlled by organised crime, nobody knew anything about trafficking for the purpose of pornography production, or the connection between trafficking for the purpose of sexual exploitation and pornography.

The consumers

Little is known about the average consumer of Internet pornography and live Webcasts. More specific information about "markets" for "adult entertainment" have been compiled by Internet research and marketing companies for sale to sex industry companies. The information gathered about workplace use of pornography is probably the best source of data there is about the general audience for adult pornography. There seems to be broad use of the Internet by many people to access pornography, with a sharp skewed distribution toward a minority of men who have developed an obsession and spend hundreds of hours downloading thousands of images.

Researchers at the COPINE Project in Ireland made the following observation about the lack of information about consumers of pornography. In this case, the authors were referring to child pornography collectors:

> "A major weakness in contemporary work in this area is that it does not consider how individual consumers use and understand pornographic or other photographic media nor does it acknowledge their choice, responsibility and accountability for their behaviours. A particular absence in the literature is any attempt to understand the nature of photographs of children, or their significance for the user."[14]

1. Rich, 20 May 2001.
2. Rich, 20 May 2001.
3. Rich, 20 May 2001.
4. Natasha Singer, "Blue Danube – The story of Budapest's booming export: the skin flick", site accessed 25 February 2001.
5. "To its buyers and sellers, the sex trade is just another busine$$", site accessed 25 February 2001.
6. Geary, March 1997.
7. Singer, February 2001.
8. Updated Company Press Release, 10 May 2000.
9. Singer, February 2001.
10. Singer, February 2001.
11. "To its buyers and sellers, the sex trade is just another busine$$", site accessed 25 February 2001.
12. Fedor Lukyanov "'Alive goods' is flown from the East", *Rosiyskaya Gazeta* (Budapest), 27 May 2000.
13. Lukyanov, 27 May 2000 .
14. Max Taylor, Gemma Holland and Ethel Quayle, 2000 "Typology of paedophile picture collections", COPINE project, Child Studies Unit, Department of Applied Psychology, University of Cork, Ireland

James McLaughlin, Keene Police Department, New Hampshire, USA, made a similar comment, once again in regard to child sex offenders who use the Internet.

> "Presently there is no profile for people who go on to the Internet and seek out child pornography, sexual contacts with children or who want to engage in cybersex with children. At this time there is not enough data collected to determine if there is any difference between those who engage in the sexual abuse/exploitation of children in traditional ways as compared to those who employ computer technology to do so."[1]

This observation is confirmed by the results of the questionnaire sent to the member states of the Council of Europe. Most of the persons contacted replied that, so far, no studies/research had been undertaken in their respective countries on persons using NITs with a pornographic/sex-related motivation, with the exception of a German study carried out in 1997 on child pornography by the Federal Office of Criminal Police in Wiesbaden, and the data from the European Centre for missing children "Child Focus".

The unintended users

There are millions of unintended users of sexually exploitative materials on the Internet. Pornographic material is so pervasive in all forums on the Internet that it is difficult to avoid it.

The sex industry uses very aggressive techniques to get and keep pornographic material in front of user's eyes. Techniques such as page jacking and mouse trapping were discussed earlier in this report. Spam – unsolicited e-mail – advertising the sex industry lands in almost everyone's e-mail inbox. In a Websence survey, one half of employees surveyed say they receive pornographic, sexist or racist e-mails at work. [2]

The sex industry is using new "push" technologies to market their products and services to everyone using the Internet. Robert Flores, formerly Deputy Director of Child Exploitation and Obscenity Unit, US Department of Justice, now appointed to head the Juvenile Justice and Delinquency Prevention Program, US Department of Justice, testified before Congress on the aggressive marketing used by the sex industry:

> "The pornography industry has also become among the most aggressive marketers on the Internet, using newly developed 'push' technologies alongside offensive and fraudulent marketing ploys. ... the explosive growth in the distribution of obscenity, aggressive marketing efforts ... assault and trap unwilling Web surfers."[3]

The future user

Teenagers are learning social norms and attitudes, and establishing viewing patterns on the Internet. The sex industry is working to be part of the mix. Pornography is considered just part of the multi-content, multi-media mix.

> "... it is ... essential for media companies and advertisers, because teenagers form media habits that will fundamentally influence their adult behaviour. ... the new habits gestating in the bedrooms of Britain's 4.4m 13- to 17-year-olds will influence the centre of gravity of media behaviour for a generation. ... Teenage bedrooms contain a lot of technology. Four out of five 13- to 17- year-olds have an analogue television in their bedroom; more than a third have their own video; almost every bedroom has a radio, too. But the most rapid growth is in interactive media. ... The Internet, too, is invading the bedroom. At least 68 per cent of 13- to 17-year-olds now have access to the Internet at home. ... almost 10 per cent have an Internet-enabled PC in their own bedroom and this percentage is rapidly rising."

The largest percentage of users of the Internet is young people. They are forming their opinions and attitudes about sexuality, about norms and acceptable practices. The sex industry knows, just as the tobacco industry does, that getting adolescents hooked is their solid link to success and lack of opposition in the future.

People's, especially teens', attitudes toward women and men, their expected behaviours, roles and rights, are being strongly influenced by the content on the Internet. Considering the misogynistic content of much of the material, it does not bode well for equality between women and men.

In order to collect more information on the users and their motives, the Group decided to conduct *further research* in this area. It suggested that Ms Hughes focus more attention on the role of marriage agencies/introduction services (sometimes referred to as mail-order-bride agencies) in the trafficking of women for the purpose of sexual exploitation, to supplement the study of the users.

The results of her study are reported below.

1. James F. McLaughlin, 1998.
2. *Workplace productivity*, 23 April 2001.
3. Flores, 23 May 2000.

B. The role of marriage agencies in trafficking in women and trafficking in images for the purpose of sexual exploitation

One of the questions that arises in considering the trafficking for the purpose of sexual exploitation of the tens of thousands of women into western Europe is how they are recruited by traffickers and/or pimps. There have been many documented cases of women being deceived by traffickers after the women responded to employment advertisements. This report addresses the involvement of marriage agencies in trafficking for the purpose of sexual exploitation.

Some NGOs consider the "bride trade" to be a form of trafficking in women for the purpose of sexual exploitation in and of itself because its operation depends on an inequality of power between men and women. The bride trade is based on recruiting women from regions of poverty and high employment, and marketing of the women based on sexual, racial, and ethnic stereotypes. The men seeking companions or wives through this route often express their desire for women who are interested in fulfilling traditional family roles. A review of the marriage or introduction agencies that operate on the Internet reveals the sometimes subtle, but often blatant, sexualised photographs of the women are used to appeal to men. The descriptions of the women claim they are oriented towards pleasing men.

There have been numerous cases in western Europe and the United States of women who met men through marriage agencies and became victims of domestic violence, and in some

cases, victims of sexual slavery. Also, there have been cases in which "mail-order brides" were murdered by violent partners. NGOs state that women who find western partners through marriage agencies are at higher risk of becoming victims of violence and exploitation, but there is not enough data or research to substantiate that.

In St Petersburg the Psychological Crisis Centre for Women reports that they have heard of women recruited by marriage agencies being trafficked into the sex industry, but they had not worked directly with such a case. They said they knew of women recruited by marriage agencies who were used as surrogate mothers, or brought to western countries while pregnant to give birth to their babies, then deported to Russia.[1]

In countries where recruitment of women by marriage or introduction agencies is popular, the general public does not understand the risk of signing up with these agencies. An NGO worker in St Petersburg said that her mother was urging her to sign up. She said her mother said, "Why waste your time with that work. Why not correspond with a western man and find a better life?" She said she knew of cases in which mothers accompany their daughters to marriage agencies to sign them up, when the daughters are too afraid to go alone.[2]

There was some indication that traffickers may use the Internet to recruit women. A report by the Denmark Police[3] noted suspicious advertisements for nannies, waitresses, and dancers on Web sites in Latvia and Lithuania. The significance of these advertisements in the recruitment of women was disputed. Some thought that so few girls and women have Internet access in Latvia and Lithuania, especially in the poor, rural areas from which many girls and women are recruited, that this could not be an effective recruitment tool. Others thought that almost all girls and women have access to the Internet through schools and libraries, where they may go to search for work abroad.[4]

The recruitment of women by marriage agencies may be a way to facilitate women's access to the Internet. For example, in Riga, Latvia, one of the largest marriage agencies in the world, has a franchise in a café. In the café, women access the Internet to correspond with men who have subscribed to the service.[5] Other marriage agencies provide Internet access at their offices so women can correspond with men who pay additional fees for conversations with women.

In these cases, marriage agencies themselves may not be involved in trafficking for the purpose of sexual exploitation, but are providing access to the Internet and contacts in the West that may increase the likelihood of women corresponding with or meeting traffickers.

1. Interview, St Petersburg Psychological Crisis Centre, 18 August 2001.
2. Interview, St Petersburg Psychological Crisis Centre, 18 August 2001.
3. This report is also mentioned in Ms Hughes' study on the users.
4. Interview, Lisbet Jörgensen, Denmark Police, 2 May 2001.
5. Jorgen Johannson, "Down at the love-trade hotel", *The Baltic Times*, 10-16 May 2001.

1. Recruitment of Women by Marriage Agencies in Countries of the Former Soviet Union

Research on Internet-based marriage or introduction agencies was undertaken to investigate the role of marriage agencies in the trafficking in women for the purpose of sexual exploitation. Since this type of research had not been done before, it was not clear at the beginning what the findings or the significance of the findings would be. The questions to address were:

- How many Internet-based marriage or introduction agencies are operating in the countries of the former Soviet Union?
- How many women have been recruited by these agencies?
- Are there certain countries, regions, and cities from which women are being recruited?
- Are these the same countries, regions, and cities from which women are known to be trafficked into sex industries?
- Are marriage or introduction agencies involved in trafficking in women for the purpose of sexual exploitation?

During summer 2001, searches on the Web found almost 500 marriage agency sites with women from former Soviet countries. Two hundred and nineteen (219) Web sites with women from countries of the former Soviet Union were indexed. A database was constructed with the following information from each Web site:

- Url of the Web site,
- Web site name,
- US or European address of the agency,
- City and country location and/or address of the agency in former Soviet country
- E-mail address, telephone and fax number
- Price for addresses of women and/or membership fee for men to join the club
- Destination of tours, if arranged by the agency.
- Additional relevant information, such as availability of video tapes or nude pictures of women, obvious connections to the sex industry

The 219 agencies that were indexed are representative of those found on the Web. They include large agencies with thousands of women listed and very small agencies with just a few dozen women listed. Agencies from diverse locations were also included, especially those outside large cities. Some agencies, the largest ones, included women from almost all of the former Soviet countries; other agencies were regional and included only women from one city or oblast.

From each of the Web sites, the number of women from each city, oblast and country was entered in the database. A total of almost 120000 women were counted from these sites. Efforts were made to avoid overcounting. There were several Web sites that compiled women from other sites or agencies. These duplications were not counted.

There was a large range of numbers of women from each country (See Table 1). The fifteen countries of the former Soviet Union can be divided into three distinct categories for the recruitment of women by marriage or introduction agencies: *High*, *Medium*, and *Low*. Although there are very large differences in the size and populations of these fifteen countries, there are still very large differences in the recruitment of women by marriage agencies in these countries.

The *High* category with the largest numbers of women were the Russian Federation with over 62000 women, followed by Ukraine with almost 32000, and Belarus with almost 13000.

There were a few *Medium* range countries with a few thousand women: Kazakhstan (3037), Kyrgyzstan (4190), Latvia (1760), and Uzbekistan (1139). The rest in the *Low* category had fewer than 1000 women: Azerbaijan (204), Estonia (551), Lithuania (626), Moldova (884); and a few countries had under a couple of dozen women, Armenia (23), Georgia (7), Tajikistan (8), and Turkmenistan (25).

Table 1: Women recruited by marriage agencies from countries of the former Soviet Union

Armenia	23
Azerbaijan	204
Belarus	12683
Estonia	551
Georgia	7
Kazakhstan	3037
Kyrgyzstan	4190
Latvia	1760
Lithuania	626
Moldova	884
Russian Federation	62605
Tajikistan	8
Turkmenistan	25
Ukraine	31837
Uzbekistan	1139
Unknown	70
Total	119649

The three countries in the *High* category (Russian Federation, Ukraine and Belarus) were categorised by the number of women recruited in each oblast on the 219 Web sites.

In the Russian Federation there were very large differences in the number of women recruited from each oblast (see Table 2). Fewer than ten women had been recruited from thirteen of the oblasts. Fewer than 100 women had been recruited from 41 of the oblasts. Only ten oblasts had more than 1000 women. St Petersburg, with by far the highest number, almost 16000, represented almost three to four times the number of women recruited compared to the next closest oblasts – Moscow with over 3600 and Volgograd with almost 4900.

Although there are considerable differences in population among the oblasts, the size of the difference in recruitment numbers most likely represents the activity of recruiters and how marriage or introduction agencies are viewed.

Table 2: Women recruited by marriage agencies in the Russian Federation by oblast

Adygea	18	Moscow	3642
Alania	4	Murmansk	43
Altai	73	Nizhniy	178
Amur	25	Novgorod	502
Arkhangelsk	253	Novosibirsk	655
Astrakhan'	429	Omsk	731
Bashkortostan	440	Orel Oblast	72
Belgorod	86	Orenburg	96
Birobijan	3	Penza	311
Bryansk	69	Mordovia	14
Buryatia	15	Perm	221
Chelyabinsk	474	Primorskiy	645
Chita	3	Pskov	55
Chukot	2	Rostov	1044
Chuvashia	154	Ryazan'	282
Daghestan	8	Sakhalin	178
Irkutsk	133	Samara	1510
Ivanovo	32	Saratov	2344
Kabardino-Balkaria	22	Smolensk	23
Kaliningrad	295	St Petersburg	15694
Kalmykia	2	Stavropol	365
Kaluga	72	Sverdlovsk	2003
Kamtchatka	27	Tambov	111
Karachay-Cherkessia	4	Tatarstan	2165
Karelia	49	Taymyr	31
Kemerovo	173	Tomsk	235
Khabarovsk	313	Tula	43
Khakassia	7	Tuva	1
Khanty-Mansi	41	Tver	1373
Kirov	26	Tyumen	159
Komi	203	Udmurtia	317
Komi-Permyak	1	Ul'yanovsk	280
Kostroma	10	Vladimir	58
Krasnodar	834	Volgograd	4897
Krasnoyarsk	175	Vologda	60
Kurgan	82	Voronezh	121
Kursk	27	Yakutia	21
Lipetsk	82	Yamalo-Nenets	2
Magadan	22	Yaroslavl	64
Mari-El	1869	Unknown	14967
		Total	62605

There were sizeable differences in the number of women recruited by oblast in Ukraine also (see Table 3). In Ukraine there are a few distinct patterns for the recruitment of women by marriage agencies. Generally, the oblasts with the lowest number of recruited women are in western Ukraine. Oblasts with large cities, such as the capital Kiev, Odessa, and Dnipropetrovsk, have large numbers of women in the marriage agencies. The Crimea has the largest number of women recruited

(5515), and the other oblasts on or near the Black Sea have fairly high numbers of women recruited from them.

Table 3: Women recruited by marriage agencies in Ukraine, by oblast

Cherkas'ka	149	Mykolayiv	533
Chernivhivs'ka	35	Odessa	3225
Chernivitsi	268	Poltava	368
Dnipropetrovsk	2742	Respublika Krym	5515
Donetsk	1055	Rivnens'ka	2
Ivano-Frankivsk	10	Sums'ka	1994
Kharkivs'ka	1188	Ternopil'	12
Khersons'ka	1053	Vinnytsya	440
Khmelnyts'ka	28	Volyns'ka	24
Kiev	3401	Zakarpats'ka	46
Kirovohrads'ka	10	Zaporizhzhya	539
Luhans'ka	281	Zhytomyr	125
L'viv	41	Unknown	8753
		Total	31837

The oblasts of Belarus also show considerable variation in the number of women recruited, with a low of 33 in Hrodzyenskaya to two oblasts, Homyelskaya and Minsk, having over 4000 (see Table 4).

Table 4: Women recruited by marriage agencies in Belarus, by oblast

Brest	202
Homyel'skaya	4905
Hrodzyenskaya	33
Mahilyowskaya	229
Minsk	4303
Vitsyebskaya	740
Unknown	2271
Total	12683

2. Sexually exploitative services offered through marriage agencies

Of the 219 marriage or introduction agency Web sites, 78 offered tours to meet women. Although most marriage agency Web sites make money by selling contact information to men, there are a few that only operate as introduction services (they don't sell addresses or facilitate correspondence). The men have to travel to the city, and then the agency will introduce them to women. While some of the agencies have a narrow focus of introducing potential marriage partners, other agencies offer pornographic and prostitution services.

A number of the Web sites provide models for pornographers. One agency offers men the opportunity to come to Russia on "erotic tours" and take pornographic pictures of the women.

Several of the Web sites include nude photos of the women. Some of the Web sites seem to be fully integrated into the sex industry. For example one Web site offers Russian brides, escort services, Russian porn, and Russian amateurs (pornographic photos of Russian women). There are links that connect to typical sex industry sites.

It is not known if any of these marriage or introduction agencies are involved in trafficking in women for the purpose of sexual exploitation into sex industries in other countries. There are a number of aspects of these types of agencies that indicate that they are likely to be involved:

- They have recruited a number of women who have indicated a desire to travel abroad or emigrate;
- The women are single and able to move, although some of them may have children;
- The women may have tried corresponding with men, meeting western men on tours at "socials" sponsored by the agencies, and now be more willing to go abroad if they agency makes them an offer.

Also, some of the agencies on the Web site are operating other businesses that facilitate the travel and trafficking for the purpose of sexual exploitation of women. In Chelyabinsk, Russia, an NGO representative said that the traffickers operate in travel agencies, with each agency specialising in one particular country where women are sent.[1] In St Petersburg an NGO representative said that marriage agencies are a well-organised business and "well-protected" legally and by the political-business-criminal networks. As in Chelyabinsk, the same people who own marriage agencies also own foreign travel and employment agencies, some of which are known to be traffickers.

As a result of poverty, high unemployment, and a belief in Western utopias, many women want to go abroad. NGOs report that in many cases once a woman decides the solution to her problems is to go abroad, she will try every agency or strategy, regardless of the risk.

1. Interview, Larisa Vasileyeva, *21st Century Women*, Chelyabinsk, Russia, 15 August 2001.

3. Marriage agencies' recruitment of vulnerable populations

There are a few marriage agencies on the Web that either specialise in or include women or girls from especially vulnerable populations. One agency offering marriage agency services is a Russian government social service agency. The Family Social Assistance Centre, a subsidiary of the Ministry of Social Assistance, has a typical marriage agency Web site linked to it. The agency, located in Rostov-on-Don, provides medial and social assistance to "families with disabled children, single-parent families, large families, and other vulnerable layers of the population." Services they provide include "psychological consulting both to children and adults," and "legal assistance to the women suffering domestic/sexual/societal" violence. The agency also provides "assistance to the lonely people inside Russia and all over the world in creating families though Internet". The link is to their marriage agency. The descriptions of the women do not say they have previously been abused, although there are a

number of women whose average age is higher than most marriage agency Web sites.

Women and orphans with disabilities are extremely vulnerable. The loss of the social supports following the collapse of the Soviet Union has not doubt severely worsened the circumstance for many.

Several of the Web sites in Russia and Ukraine have underage girls listed as potential correspondents or wives. There are also Web sites offering introduction services and pornography of women with disabilities. The photographs on the Web site range from modest to sexualised. The descriptions of the women often include pledges of loyalty to a man who will take care of them. On the same Web site are photographs of orphans with disabilities. Viewers are urged to send gifts or adopt them

It is difficult to know how many of these agencies are providing the services they claim of selling addresses, and how many are involved in the activities that meet the criminal definition of trafficking in women for the purpose of sexual exploitation. Certainly, most are promoting the sexual exploitation of eastern European women by western men.

4. Trafficking in images for the purpose of sexual exploitation

There have been numerous reports to NGOs in all parts of the world of nude or pornographic images of women being put on the Internet without their permission and with harmful intent. Some law-enforcement agents who specialise in cybercrime are becoming increasingly aware of the harm done to victims by the new technologies. An official at the Internet Monitoring Service, National Police Headquarters, Hungary said the following about the use of new technologies for the trafficking in women for the purpose of sexual exploitation:

> "I think this is a serious enough problem, that needs attention, it must be dealt with. It is already clear that certain groups of criminals begin to realise the importance of this issue, and use this technology not only on the level of trafficking in human beings for the purpose of sexual exploitation, but also on the level of domestic exploitation of the victims as well."[1]

At this point, most of the incidents that have been documented would be considered part of domestic violence. The men posting the images are usually former partners of the women who are attempting to harm or blackmail the victim. Two examples follow:

In St Petersburg, Russia, the former partner of a woman posted a photograph of the woman with a message and contact information in several locations on the Internet. The contact information was correct, so the woman received many calls from men asking to meet her for sex. She reported this to the police, and they laughed. She asked the St Petersburg Psychological Crisis Centre for Women for assistance, but they could not get the police to take the case seriously or to intervene for the victim.[2]

In Bulgaria, a program to assist victims of domestic violence received a report that a woman's former partner blackmailed her by posting nude photographs of her on the Internet.[3]

An NGO in Denmark who works with victims of prostitution, pornography, and trafficking for the purpose of sexual exploitation described the harm done to women. They say that the new capabilities of the Internet further the harm to victims.

> "Contact with victims of prostitution, porn and trafficking for the purpose of sexual exploitation has given us information on the long-term harms done to people having been projected on the Internet. Pictures and video films never grow old and can be found on the Internet many years after the actual person has stopped acting in this business, which is seriously violating the person involved. The psychological damage done to victims in this ways is very harmful. You can find pictures 20-30 years old while surfing the web, also images of children being abused. Adults can in that way find pictures of themselves being sexually abused as children many years after the abuse has stopped. And they have no possibility to get these images removed from the Internet, even when they know where they are shown."[4]

St Petersburg, Russia has become a centre for the production of pornography since the end of the Soviet Union. Representatives from NGOs report that they have heard of many cases of women being forced to make pornography. They say the police will take complaints only if children are used in pornography. Therefore the centre can only offer the women psychological counselling, not legal assistance. Many of the women in prostitution in St. Petersburg have also been used to make pornography.[5]

The multi-function agency described above gives this contradictory message to men who are paying to have nude photographs taken of women:

> "These pictures will be taken by one of our female photographers. None of these pictures will appear anywhere on Internet. The agency is not liable for any use of the photos purchased by you if you request to give copies to ladies. You understand and agree that ladies can post these photos on our web-site or on web-site of any other agencies and also send them to other men."

The agency seems to be indicating that once the photographs are taken, they can use them in any way the agency wants, although control is attributed to the woman. In reality the woman has little, if any, control of the photographs that have been taken of her.

Through the use of new technologies, new sex-related businesses are opening up that will facilitate the trafficking for the purpose of sexual exploitation of images of women.

The following is a case in which the owner plans to open a pornographic Internet business in Latvia, Lithuania, Hungary, and possibly Russia. An American NGO representative posing as a potential business partner obtained this information.[6]

The following is the businessman's description of the proposed Internet live Web cam:

> "After 10 years on the internet ... we are now going into the highly lucrative LIVE WEBCAM business. This is an opportunity for you to share in an area of the Internet that makes an incredible amount of money ... the Adult Industry! The creation of a website on the Internet that would

1. Tibor Pszleg, National Police Headquarters, Internet Monitoring Service, Hungary, Spring 2001.
2. Interview, St Petersburg Psychological Crisis Centre for Women, 18 August 2001.
3. Nada Kozhouharova, Animus Association, Bulgaria, Spring 2001.
4. Reden, International Abolitionist Federation, Denmark, Spring 2001.
5. Interview, St Petersburg Psychological Crisis Centre for Women, 18 August 2001.
6. Ken Franzblau of Equality Now.

allow viewers to see, talk and play online with young, beautiful women from Eastern Europe. This website is the first of many (approximately 200) websites that this project will set up throughout Eastern Europe, making the company the largest website chain of its kind on the Internet. This is truly Internet history in the making!" [11 July 2001]

Businesses of this sort involve placing multiple cameras that broadcast directly to the Internet in every room of a house so that voyeuristic men can watch women who live there all the time. The following is the promoter's description of his proposed business:

"Additional features of this business are private conversations and sessions with the women. The women are expected to perform private sex shows for the viewers."

The sexual or pornographic nature of the "private chats" is revealed if you consider that the need for translators is never mentioned.

The following are the list of products and services the business expects to sell to a western market: as with the marriage agencies, this business expects to market tours for the men to travel to the eastern European cities to meet women. Aside from the revenues derived from memberships and chat lines, the models will be promoting and selling:

- Their individual videos. Each model will have at least 10 personal videos to sell.
- Their personal lingerie and underwear.
- Trips for website members to meet the girls.
- Personalised 15-second Strip-O-Grams that can be sent via e-mail.
- Gifts that members purchase for the girls (flowers, perfumes, toys, etc.)
- Personalised erotic videos that the models record and perform on a per-order basis [11 July 2001]

The NGO representative who posed as the potential business partner was interested in obtaining information about the women would be treated. He formulated his questions to give the impression he was interested in protecting his investment by making sure the women performed well.

"There will be 7 beautiful girls living in the house at any given time. The girls will be changed every 3-4 months to provide members with fresh faces, assure their loyalty to the website and generate repeat business. We intend to replace the girls every 3-4 months, with the exception of the top money-makers – we will of course, keep them. The reasoning behind this is to promote loyalty with our paying members – they will keep coming back if they know that they will see new girls every so often. By your question about guarantee – if this means can we find girls – the answer, of course, is yes. There are thousands of girls there that would love to have this job. For instance, two weeks ago, we called for a casting in Riga – something that was organized on the spur of the moment by an agent, and we had over 200 applicants – all of them beautiful!" [11 July 2001]

When the NGO representative pressed for more information on how he could ensure that the women performed to men's satisfaction, this was the response:

"You have to understand the social situation in Eastern Europe. These girls respect authority, as they are used to it. There is such a demand for work over there that the girls will not jeopardize a 'cushy' job such as this, where they can make a lot of money. Girls know that they can be very easily replaced. The average salary anywhere in Eastern Europe is about $100 a month, so the girls are being paid premium money. These girls work hard – because they are ambitious enough to know that they will be rewarded if they do. They are not spoiled brats – at least, not yet – compared to western girls. One very obvious quality that they have, which is starting to fade in the west, is that the girls there are very feminine." [11 July 2001]

According to a modelling agreement the business owner said he was going to have the women sign, they are required to work a minimum of 60 hours per week. The work schedule is entirely under the control of the producer. The producer can terminate the contract before the end of the time period, but not the woman. The producer has the right to withhold the woman's pay. The woman can be forced to pay "damages" if she does not perform adequately or breaks the contract. Considering that there is a two-week delay in payment for services and a 30-day delay in payments of commissions, if the woman violates the contract in any way specified by the producer, she will not receive the money she has earned. The agreement also gives the producer the right to use images and videos made of the woman in any way he chooses. In the agreement it also states that the producer will post "rules and regulations" that must be followed. In brothels and escort services there is often a long list of rules aimed at controlling the women. The rules are often so restrictive that it is difficult to avoid breaking some of them. The fines are often very high. The goal is not only control of the women, but a way to deny full compensation to the women. If the women are not paid fully one week, they can become indebted, or further indebted, to the pimp, thereby preventing them from leaving.

The following are business details about the Internet business, which include references to political protection:

"Producer shall incorporate this project offshore, and banking and revenue disbursements shall come from an offshore account. As in the United States, independent contractors are outside the scope of regular employment. Further, no one really pays attention to these things in Eastern Europe. As long as the company pays taxes (and believe me, probably 70% of the companies there do not), no one will bother you. Also, I told you before that we have excellent connections there, which include both government and public." [19 July 2001]

5. Conclusion

As was mentioned in the introduction, the information gathered is partial, but there are strong indications that at least some marriage agencies and introduction services are involved in the trafficking in women for the purpose of sexual exploitation. It is important in the future to be able to document a few cases of trafficking for the purpose of sexual exploitation that go beyond domestic violence to trafficking for the purpose of sexual exploitation for the sex industry. With such evidence, the case could be made for including marriage agencies in trafficking for the purpose of sexual exploitation prevention and awareness programs. A problem subsequent to connecting marriage agencies to the trafficking in women for the purpose of sexual exploitation is getting lawmakers and law enforcement agencies to act against it. In Russia, there is no law against the trafficking in human beings for the purpose of sexual exploitation. In Ukraine, quite adequate laws against trafficking for the

purpose of sexual exploitation have been passed, but there is weak enforcement.

A response to the trafficking of pornographic images of women raises steep challenges. There would be no problem in getting cases in which women claim that images have been made against their will. Neither would there be a problem finding women who claim nude or pornographic images of them were posted on the Internet against their will. The problem is that women have not been able to get law enforcement or the courts to agree that harm has been done or that legal action can or should be taken.

One of the exceptions to this general attitude of the courts is Judge Jean-Jacques Gomez's ruling earlier this year in the case in which an actress sued to have pornographic photographs taken of her years ago removed from the Internet. He ruled in the woman's favour saying that she did have a right to have the images removed, even though she had signed a contract when the photographs were taken. The case was being appealed.

Although trafficking in women for the purpose of sexual exploitation and the trafficking in images for the purpose of sexual exploitation are very closely related, if not the same thing, they are viewed and treated very differently. Internationally, there has been progress in raising awareness and acting against the physical trafficking in women for the purpose of sexual exploitation. Unfortunately, the trend has been just the opposite for trafficking in images for the purpose of sexual exploitation. Most people see the reduction or elimination of prosecution of adult pornography as being a victory for the individual rights of people and an end to suppressive government enforcement of morality based laws. They assume all women in pornography are consenting, even when the women are visibly injured. If a woman protests after a photograph has been taken or a video made, people assume she consented at the time, but now is embarrassed by other people seeing it. Or they blame the victim and say she shouldn't have been so silly as to allow such photographs to be taken in the first place.

In connection to the use of new technologies, there is fatalistic assumption that nothing can be done when it involves the Internet. Because of the libertarian culture on the Internet and the lack of intervention in the past, people have developed the attitude that it is not possible to stop anything. This view is promoted by the sex industry and Internet industry as well. They have broadcast the message so often that the Internet cannot be "censored," that most people believe it is impossible to intervene in any way.

Although new techniques are being developed all the time through communications and information technologies, the basic challenge remains the same – how to ensure the right of human beings to be free of sexual exploitation. Technology is providing new ways to traffic women for sexual exploitation and new ways to transmit the images of sexual exploitation. The new technologies present new challenges to lawmakers, law enforcement, and international cooperation, but the problem cannot be solved in cyberspace without solving the problem in every local community. It is only when basic human rights, including the right to be free of violence and sexual exploitation, are ensured to all people that the problem will be solved.

The challenges

Trafficking in human beings for the purpose of sexual exploitation through the use of the Internet offers huge and grave challenges to society, from law-makers to law enforcement, to NGOs.

Incompatibility of laws among states, and sometimes, even within states, is a challenge. And there is probably no other area with such diversity of, even opposite, policies and practices, as prostitution, pornography, and trafficking in human beings for the purpose of sexual exploitation. One policy decision that hinders the actions to combat sexual exploitation on the Internet is making economic growth and development of the Internet a priority, and to do nothing to impede e-commerce.

Denial of the harm

Since this is a report on the users, it focuses on the challenges to combating men's women and children sexual exploitation. The biggest problem in combating trafficking for the purpose of sexual exploitation is the denial of the harm to women and children.

There is deep, pervasive denial of the harm of sexual exploitation throughout the world. The sexual exploitation of women has been normalised by the sex industry. There are massive amounts of pornography readily available on the Internet, with no limits on how transgressive, violent or degrading the images are. The women are always smiling, implying that they are consenting and enjoying the acts, even when they are painful and humiliating.

The users who sexually exploit women and children defend their rights and actions. They frequently portray themselves, even child sex abusers, as victims of oppression and intolerance. In the users' view, groups opposing sexual exploitation and even child pornography are attempting to oppress the users' right to pursue their pleasure and express their "love" for children.

Society has become accepting of these images of sexual exploitation, and no longer questions them. Men and women, who do not have an understanding of the implications of some images, can easily come to believe that any and all sex acts are acceptable and enjoyable to women. Even law enforcement officials dedicated to fighting trafficking in human beings for the purpose of sexual exploitation often use pornographic language and terms to describe what is done to the women and children. In doing so they become complicit with the traffickers and users in the denial of the harm by minimizing or eroticising the actions of the perpetrators.

Disconnection between acts and images

One of the fundamental questions that this inquiry addresses is the connection between the physical trafficking in human beings for the purpose of sexual exploitation and the images produced of those crimes. In the areas of sexual exploitation there is a strong disconnection between acts and images. Only in child pornography has the link between acts and image been maintained, with an image being considered the pictorial evidence of abuse. Asking the question about the impact of the use of information technologies on trafficking in human beings for sexual exploitation takes us to the links between acts and images.

Perpetrators and profiteers of sexual exploitation will argue strongly for maintaining the disconnection between acts and images. Human and women's rights advocates and those defending the democratic rights of citizens to dignity and freedom have to connect the acts and images. Asking about the use of new technologies and trafficking for the purpose of sexual ex-

ploitation takes us into cyberspace, a place that seems to exist without physical embodiment, but in fact is a very real, physical network of electronic components, wiring, cables, and program code. The images and videos of sexual exploitation that are found on the Internet have just as much basis in reality as cyberspace. With the exception of virtual or animated images, every image is produced by recording the acts of real people.

The challenge is to change attitudes, policies and laws that connect the acts and images in ways that preserve rights of freedom of expression, but protect the rights human beings to be free of criminal acts of trafficking for the purpose of sexual exploitation.

II. Existing legislation in the different member states and the relevant international instruments

A. At national level

The legal and legislative aspects are crucial for effective action against damaging use of new information technologies. This is the reason why the group decided to gather all available information on countries' legislation concerning the Internet and its unlawful and improper use. A questionnaire on the legal framework, law enforcement and anti-trafficking for the purpose of sexual exploitation actions and cases, sent to all the member states, sought to determine the state of existing legislation and its limits at national level and the role of the law in combating illegal or damaging use of the Internet.

After gathering and analysing the information obtained through the questionnaire, one can say that the legislations currently in force in the member states of the Council of Europe do not regulate the use of Internet in connection with trafficking in human beings for the purpose of sexual exploitation; few national legislations tackle the issue of the Internet content and the question of trafficking for the purpose of sexual exploitation separately, and the questions remain disconnected. As Ms Hughes described it in her study on the users:

> **"when the content or activity is sexual there is no consensus, no norms, and no homogenized laws to set a standard. What is legal in one country is illegal in another. Even laws that criminalize certain activities focus on different actions."**

Internet law hardly exists, and the difficulty of establishing such an area of law is increased by the fact that Internet goes beyond national boundaries.

Experts also underlined that there was a gap between cases concerning children and child pornography, clearly prohibited by most European laws, where Internet content providers had been asked to close Internet sites, and cases involving trafficked adults or mail order brides, where the laws were less clear and the actions taken less effective.

Even if the preparation and adoption of adequate legislation was deemed essential, the importance of analysing the means of implementing such legislation, which otherwise would remain only a token gesture, was also underlined. It was also stressed that there seems to be a decrease in prosecution. Ms Hughes stated in her study on the role of marriage agencies that a problem subsequent to connecting marriage agencies to the trafficking in women for the purpose of sexual exploitation is getting lawmakers and law enforcement agencies to act against it:

> "Internationally, there has been progress in raising awareness and acting against the physical trafficking in women for the purpose of sexual exploitation. Unfortunately, the trend has been just the opposite for trafficking in images for the purpose of sexual exploitation."

Consequently, the Group agreed that it was important to study the *cases* already resolved, even if they often included qualified information: the aim was to study the techniques used in order to draw conclusions which could be generally applicable. Also it decided to follow closely the case concerning LICRA and UEJF v. Yahoo! Inc. and Yahoo France.

The group considered the information on the existing legislation on Internet in the member states concerning the technical aspects, the content, the financial aspects, the link with trafficking for the purpose of sexual exploitation and mandated the Swiss Institute of Comparative Law (SICL) in Lausanne to provide a comparative study on the existing national legislations of nine countries – Belgium, France, Hungary, Italy, Moldova, the Netherlands, Russia, Sweden and Switzerland – concerning criminal liability for acts committed through the Internet in connection with the trafficking in human beings for the purpose of sexual exploitation. The SICL was asked to specifically take into account following aspects: the trafficking in human beings ("slave trade"), the Internet, prostitution, pornography, money laundering and matrimonial agencies ("mail-order bride businesses").

This study mainly concerns the penal legislation – the Penal Codes themselves as well as provisions of other laws which contain penal sanctions and the Criminal Procedure Codes – of the above-mentioned countries. Only the specific legal provisions have been examined, the statistical aspects or the implementation and application of these judicial norms have not

been treated. The study concentrated on national law, namely criminal law and criminal procedure law as well as the relevant jurisprudence in this field. With respect to national law, draft legislation which has arrived at a parliamentary stage was also mentioned. Due to the diversity and vagueness of the doctrine and debates, as well as the proliferation of soft law concerning the subject it was decided that these issues would be beyond the scope of this report, notwithstanding the fact that these issues – the latter in particular – are rather important for Internet related matters. One exception has been made: a brief discussion of some aspects of Belgian soft law deemed of particular interest by the experts was included in the study.

The tables and the general conclusions are included in this report. The tables present the existence of legislation, followed by an enumeration of such legislation where it exists. The conclusions present a brief discussion of some of the major tendencies in the laws of the countries studied, as well as some specific remarks and proposals concerning possible approaches to regulations in this area. Another part not included in this report presents more detailed explanations of the legal framework of each country.[1]

1. See document EG-S-NT (2002) 2, *Comparative study on legislation on the use of Internet for the purpose of sexual exploitation*, Swiss Institute of Comparative Law, Lausanne.

Table 1: Internet: criminal liability of intermediaries and procedural measures

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
Seizure and blocking of data (Art. 39 bis CPC) Extra-territorial research on the Web (Art. 88 ter CPC) Access to encrypted data (Art. 8 quater CPC) Obligation to maintain files of identification data of users of telecommunication services (Art. 109 ter of the law of 21 March 1991)	Access to encrypted data (Art. 230-1 to 230-5 CPC) Cryptology service providers are required to provide unencryption keys (Art. 11-1 of law No. 91-646, of 10 July 1991 concerning the secrecy of messages transmitted by way of telecommunication) Penalties for refusal to cooperate in respect of unencryption (Art. 434-15-2 PC)	No specific penal legislation concerning the Internet	No specific penal legislation concerning the Internet, or concerning the liability of the various persons active on the Net	No specific penal legislation concerning the Internet	Rendering data inaccessible (draft law: Art. 125o CPC)	No specific penal legislation concerning the Internet	The law of 2002 on electronic commerce offers broad exoneration to technical intermediaries from all liability (Art. 19). The supplier of electronic bulletin board services, however, has an obligation to monitor the content of messages posted and to eliminate illicit messages (1998 Act on Responsibility for Electronic Bulletin Boards)	No specific law addressing the liability of providers. Obligation to maintain files of identification data of users of telecommunication services (law concerning the monitoring of telecommunications, in force since 1 January 2002)

Table 2: Trafficking in persons (slave trade)

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
No specific provisions; however, related provisions exist elsewhere: Law of 13 April 1995, which provides for criminal penalties for slavery and child pornography amending the following: Prostitution of minors (Art. 379 PC) Living on the earnings of the prostitution of another person (Art. 380 PC) Access to the territory, visits, residence and deportation of foreigners (Art. 77 bis, law of 15 December 1980)	No specific provisions; however, related provisions exist elsewhere: Traffic in persons for sexual purposes (Art. 225-5 et seq. PC) Traffic in persons other than for sexual purposes concerning labour (Art. 225-13 PC) The purchase or sale of a child in connection with an adoption (Art. 227-12 PC) Traffic of foreign persons (Art. 20 bis of the ordinance concerning foreigners of 2 November 1945)	The following specific provision exists: Trafficking in human beings (section 175/B PC) Related provisions: Alteration of family status by sale or purchase (section 193 PC) Constraint (section 174 PC) Promotion of prostitution (section 205 PC) Living on the earnings of the prostitution of another person (section 206 PC)	The following special provisions exist: Traffic in women for the purposes of prostitution (Art. 3 No. 6 law 1958/75) Traffic in minors for the purposes of prostitution (Art. 601, al. 2 PC) Slavery and slave trade (Art. 600 to 602 PC) Smuggling of persons into the state for the purposes of prostitution (Art. 12 legislative decree 1998/286)	The following special provisions exist: Slavery and traffic in slaves (Art. 164 PC) Pandering and sale of persons (Art. 232 PC) The sale, purchase or traffic of children for any purpose (Art. 215 PC) Taking children out of the country illegally (Art. 216 PC)	The following special provisions exist: Traffic of human beings (Art. 197a PC) Slavery and slave trade (Art. 274-278 PC) Traffic in persons for sexual purposes (Art. 250a PC)	The following special provisions exist: Trade in minors (Art. 152 PC) Substitution of a child (Art. 153 PC); illegal adoption (Art. 154 PC)	The following special provisions exist: New provisions specifically prohibiting the traffic in persons (in particular women and children) for the purposes of sexual exploitation (Art. 1a, chapter 4, of the PC, introduced 29 May 2002)	The following special provision exists: Traffic in persons for sexual purposes (Art. 196 PC)

Table 3: Prostitution

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
Although prostitution is not *per se* illegal, the following articles exist in the PC: Prostitution of minors (Art. 379) Simple and aggravated living on the earnings of the prostitution of another person (Art. 380) Soliciting (Art. 380 bis) Advertising to facilitate the prostitution of a minor (Art. 380 ter §1) Living, by an association, on the earnings of the prostitution of another person (Art. 381) Additional penalties for the commission of a crime against a minor (Art. 382 bis) Protection of witnesses (Art. 706-57 to 706-63 CPC)	Although prostitution is not *per se* illegal, the following articles exist in the PC: Art. 225-5 to 225-12 PC (most recent amendment to the law of 4 March 2002 inserting, after Articles 225-12 *et seq.* PC a new section entitled Obtaining sexual services from a minor by payment of value)	Although prostitution is not *per se* illegal, the following articles exist in the PC: Promotion of prostitution (section 205) Living on the earnings of the prostitution of another person (section 206); pandering (section 207)	Although prostitution is not *per se* illegal, the following articles exist in the PC: Law on the exploitation of prostitution No. 1958/75 (Art. 3 and 4) Prostitution of minors (Art. 600-bis PC) Tourism connected with the prostitution of minors (Art. 600-quinquies PC)	There is criminal liability for: Prostitution (Art. 231 PC) Pandering and sale of persons (Art. 232 PC)	Although prostitution is not *per se* illegal, the following article exists in the PC: Article 250a PC: "forced" prostitution (section 1) Soliciting prostitution (section 2) Living on the earnings of the prostitution of another person (sections 4 and 6) Prostitution of minors (section 5)	Although prostitution is not *per se* illegal, the following articles exist in the PC: Involvement in forced prostitution (Art. 240) Organisation or maintenance of dens for engaging in prostitution (Art. 241)	Although prostitution is not *per se* illegal, the following articles exist in the PC: Living on the earnings of the prostitution of another person (Art. 8 and 9, ch. 6) Purchase of sexual services (law 1998: 403)	Although prostitution is not *per se* illegal, the following article exists in the PC: Exploitation of sexual activity/incitement to prostitution (Art. 195 PC)

Table 4: Pornography

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
Pornography (Art. 383 PC) Representation of minors (Art. 383 bis PC) Public outrage (Art. 384 PC) 16-year-old minor as spectator (Art. 385 PC) Minor as spectator in a public place (Art. 387 PC)	Dissemination of images contrary to public decency, Art. R 624-2 PC Child pornography endangering minors: Minor an active participant (Art. 227-23 PC) Minor a mere spectator (Art. 227-24 PC)	Obscenity (section 209 PC) Display of sexuality of minors in a gravely indecent manner or exposure specifically for the purpose of arousing sexual demeanour (section 195/A PC)	Obscene publications and theatrical productions (Art. 528 PC) Pornography concerning minors (Art. 600 ter et 600 quater PC)	The manufacture or sale of pornographic materials (Art. 234 PC)	Pornography (Art. 240 PC) Minor under 16 years old as spectator (Art. 240a PC) Child pornography (Art. 240b PC) Virtual child pornography (bill approved by the Dutch Parliament on 9 July 2002)	Illegal distribution of pornographic materials or objects (act or display of sexuality in a gravely indecent manner or exposure specifically for the purpose of arousing sexual conduct, Art. 242 PC)	Manufacture and dissemination of child pornography and the representation of sexual acts committed with violence or by force (Art. 10a-b, ch. 16, PC)	Possession, manufacture and dissemination of images and objects relating to hard core pornography (i.e. pornography involving children, animals, excrement or violence) (Art. 197 PC)

Table 5: Matrimonial agencies (marriage brokers/mail-order-bride business)

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
Law of 9 March 1993 providing for regulation and supervision of the activities of matrimonial agencies and marriage brokers. Article 10 ter of the preliminary title of the CPC (extraterritoriality clause)	Law 89-421 of 23 June 1989, Art. 6 and 9 (marriage brokers) Decree 90-422 of 16 May 1990	Domaine non réglementé	No specific legislation Obligation to obtain a license	Unregulated area	No specific criminal provision Hoge Raad's Judgment (Dutch cassation court) of 7 April 1998: service of arranging fake marriages falls under the scope of Art. 197a PC (trafficking of human beings)	Unregulated area	Unregulated area	No criminal provisions Art. 406a-h of the Code of Obligations, which contains provisions concerning both government authorisation and supervision of the agency which offers the conclusion of a marriage where a foreigner is involved.

Table 6: Money laundering

The abbreviations PC *and* CPC *used in the table refer to the Penal Code and Criminal Procedure Code, respectively, in each country*

Belgium	France	Hungary	Italy	Moldova	Netherlands	Russia	Sweden	Switzerland
Law of 11 January 11 1993 concerning the prevention of the use of the financial system for the purposes of money laundering	Simple and aggravated money laundering (Art. 324-1 *et seq.* PC) Obligations relating to the fight against money laundering (Art. L 51-1 of the Monetary and Financial Code)	Criminal liability for financial operations with money illegally obtained (section 303 PC)	Criminal liability for money laundering (Art. 648 bis and 648 ter PC)	Criminal liability for performing financial operations with illegally obtained money or other goods, as well as for using these resources for performing legal economic activity or other economic activity (Art. 266 PC)	Criminal liability for money laundering (Art. 420 bis, ter, quater PC)	Criminal liability for: Illegal banking activity (Art. 172 PC) Legalisation of money (money-laundering) or of any other assets acquired illegally (Art. 174 PC)	1993 Act concerning measures against money laundering	Art. 305 bis PC (money laundering) applicable to crimes punishable by imprisonment of at least one year

1. Major tendencies of the relevant legal frameworks sexual majority

Ms Hughes noted in a study on the users:

> "At first it seems as if, at least, a line has been drawn at child pornography, but only pornography of pre-pubescent and early adolescent children has been prosecuted. Law enforcement officials cite the difficulty in determining the age of post-adolescent teens in still images and videos, so no action is taken against them."

Each country has its own definition of sexual majority, which is in some cases different from the age used to qualify pedo-pornographic crimes and certain states require a lower age than the 18-year age-limit in national legislation regarding child pornography, as shown by the table below. But there is a general tendency to increase this age up to 18.

Table 7: Age used by legislation against child pornography

Country	Sexual majority	Age used by legislation against child pornography
Australia	16-18	16
Austria	14	14
Belgium	16	18
Denmark	15	15
Finland	16	15
France	15 [a]	18
Germany	14	14
Greece	15	18
Ireland	17	17
Italy	16	18
Luxembourg	16	18
Netherlands	16	16 [b]
Portugal	---	18

Table 7: Age used by legislation against child pornography

Country	Sexual majority	Age used by legislation against child pornography
Spain	13	18
Sweden	15	18
United Kingdom	16	16
United States	---	---

Source: INHOPE, Association of Internet Hotline Providers in Europe

a. See Table 8, French legislation.
b. Will soon be increased to 18.

Table 8: French legislation

	Sexual assault without violence or coercion	
	person of full age	ascendant or person abusing a position of authority
minor under 15	Article 227-25 of the Penal Code – Prohibition	Article 227-26 of the Penal Code – Prohibition and aggravating circumstances
non-emancipated minor aged 15-18	unregulated	Article 22-27 of the Penal Code – Prohibition

As regards child pornography, the group considered that it was important in the definition of trafficking for the purpose of sexual exploitation to mention the age up to 18. It should be noted that the recommendations of the Council of Europe[1] propose that protection of children should include all boys and

1. Recommendation No. R (2000) 11 on action against trafficking in human beings for the purpose of sexual exploitation; Recommendation Rec (2001) 16 on the protection of children against sexual exploitation.

girls up to the age of 18 in all countries, and that states should make acts which constitute trafficking in children up to the age of 18 for the purpose of sexual exploitation criminal offences under their penal legislation.

2. Major tendencies of the relevant legal frameworks

General remarks

In every country examined by the legal experts of the Swiss Institute of Comparative Law, trafficking in persons, especially in women and children, is recognised as being a problem. There is not always a specific provision in the criminal legislation prohibiting the traffic in persons, however, it is sometimes deemed to fall within the definition of other more general crimes. The current trend is to introduce a specific norm which defines the traffic in persons as a criminal offence in and of itself because existing norms are not sufficient. Where there is such a specific provision, there is a clear intention to punish the trafficking in human beings for the purpose of sexual exploitation, but the exploitation for other purposes is not regularly included in the prohibitions.

Regarding prostitution, among the 44 member states of the Council of Europe, there are different legal systems or practices. Some states apply "prohibitionism" (prostitution is prohibited and clients are punished); others practice "legalism" or "regulationism" (the exploitation of the prostitution of persons of full age is not punishable) or again an "abolitionist" system (prostitution is not an offence but its exploitation is). The act of prostituting oneself is generally not punishable. The one exception is Moldova, where professional, as opposed to casual, prostitution is illegal. Incitement to prostitution, however, is a criminal offence in all of the countries researched. In Sweden also the purchase of sexual services is punishable, and in France only the purchase of sexual services of a minor is prohibited. In the Netherlands, prostitution was legalised. Moldova, on the one hand, and the Netherlands, on the other hand, represent the opposite ends of the spectrum.

There appears to be no standard concerning the legality of pornography in general, and punishable offences related thereto vary considerably from country to country. Child pornography, however, as well as pornography depicting acts of violence (so-called "hard" pornography), is punishable in each of the countries examined. Only in the Netherlands the Parliament approved a bill that will also penalise virtual child pornography. Traditionally, that which was punishable in connection with pornography was the manufacture, sale and/or distribution. Mere consumption was not illegal. Most countries have recently enacted legislation prohibiting the possession of hard pornography – a major step towards the prohibition of consumption. Under such legislation, although surfing on the Internet and viewing pornographic images is not punishable, downloading the same material is deemed to be effective possession and is therefore a criminal offence.

The research has revealed no penal provisions concerning trafficking in persons which specifically target matrimonial agencies. In some countries, like Belgium, France and Switzerland, special provisions were found in the civil legislation regulating the conditions of contracts with a matrimonial agency with a view towards avoiding abuses and overly hasty decision-making. In Switzerland, in particular, the activities of those who accept professional mandates whose purpose is the conclusion of a marriage or a partnership are subject to government supervision where such marriage or partnership involves a foreigner.

In the field of money laundering, criminal provisions formerly concerned only drugs and organised crime. The recent trend is for these provisions not to be subject to such limitations, but rather to have them apply to many, if not all, types of crimes including the trafficking in human beings for the purpose of sexual exploitation.

Specific remarks concerning Internet law

It should be noted that Internet law, or cyberlaw, as it is sometimes referred to, is an area which is fragmented and even chaotic. This domain is not regulated in a coherent and systematic way, due to the rapid pace of development of the technology, the lack of technical expertise of the legislator and/or political pressure.[1] Cyberlaw is changing very quickly and represents a dynamic and unstable area to which it is often difficult to determine which legal norms apply. It would not, however, be correct to speak of a legal vacuum even in jurisdictions in which there is no general legislation specifically concerning Internet related matters since most of the already existing relevant provisions are, at least in principle, applicable. The Internet is one of many instruments used both for communication in general as well as in connection with the commission of crimes. As a basic principle, crimes which are punishable offline are also punishable online and therefore the criminal norm should be applicable in principle regardless of whether Internet was used as a means to commit the crime – that is to say neutral with regard to the technology used.

The difficulty in prosecution of crimes committed over the Internet is not so much an absence of specific legislation, but rather a difficulty in applying existing norms to a technology that did not exist at the time the legislation was drafted. The transient and intangible nature of the Internet, as well as the anonymity and secrecy that communications via the Internet permits, make the identification of the author and/or intended recipient of an illicit communication, as well as the collection of evidence, much more difficult and elusive. This is one of the reasons why government authorities, especially in Belgium, France and the Netherlands, now tend to concentrate their legislative efforts towards adapting procedural and investigative tools to the specificities of the new technology.

It should also be noted that Internet related crimes are to a very large extent international matters since the Internet does not recognise political or national borders. As agreed in the terms of reference the experts of the SICL did not concentrate their research on international instruments notwithstanding this international dimension. Nevertheless they deemed it important to mention two such instruments in this context.

1. A problem recognised by many, including certain politicians themselves. The following example is from Belgium: *Lors de la discussion du problème de l'audition des mineurs devant la commission de la Justice du Sénat, le ministre a en revanche regretté «que l'on règle à la hâte» ce problème. Ceci pour indiquer que la loi [N.d.l.r. la loi de 1995 relative aux abus sexuels commis sur des mineurs] a été votée dans la précipitation et présente manifestement des incohérences, des erreurs, voire de difficultés sérieuses d'application.* Citations omitted.
«Le droit pénal spécial belge à l'épreuve du crime organisé», Alain De Nauw et Filip Deruyck, *International Review of Penal Law,* Vol. 69, 1998, p. 105.

The first is the **Directive of the European Union 2000/31/CE of June 8, 2000,** which among other things, target the responsibility of the technical intermediaries. In accordance with the underlying principles of this directive, access providers are not liable for information transmitted over the Internet unless they have initiated the communication, have selected the receiver, or have modified the information transmitted (Art. 12). Service providers are not liable for information transmitted unless they have actual knowledge of illicit content or, once they become aware of such illicit content, they do not act promptly to remove such content or to block access to it (Art. 14). Article 15 of the directive prohibits member states from imposing a general obligation of surveillance on these entities over the information which they transmit or store. Member states are also prohibited from imposing on them a duty to actively search out illegal content which they might host or transmit. As a result, they are totally exonerated from liability unless they have actual knowledge of illegal content which they may store or transmit. This directive has been implemented in Sweden, but has not yet been implemented in Belgium, France and Italy, despite the fact that the deadline for implementation (17 January 2002) has passed. Under these circumstances, the provisions of the directive could have direct effect if they are deemed to be sufficiently clear and precise, which appears to be the case.

The second instrument is the recent (2001) **Convention on Cybercrime of the Council of Europe.** The Convention deals, in particular, with offences related to copyright violations, computer related fraud, child pornography (Article 9)[1] and offences connected with network security, but not with trafficking in human beings for the purpose of sexual exploitation. It also covers a series of procedural police powers such as searches and interception of material on computer networks. Its main aim, as set out in the Preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation". This convention was signed by all of the states included in the study, except Russia. The convention has been ratified for the moment by two countries (Albania and Croatia), but some of these countries have already prepared drafts of implementing laws, France in particular.

1. **Article 9** – *Offences related to child pornography*
   1. each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionnaly and without right, the following conduct:
   a. producing child pornography for the purpose of its distribution through a computer system;
   b. offering of 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 pronography in a computer system or on a computer-data storage medium
   2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:
   a. a minor engaged in sexually explicit conduct;
   b. a person appearing to be a minor engaged in sexually explicit conduct;
   c. realistic images representing a minor engaged in sexually explicit conduct.
   3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
   4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1 (d) and 1 (e), and 2 (b) and 2 (c).

General proposals

A significant problem is the consent of a person to be brought into another country to work as a prostitute. Because of the extremely poor living conditions in the countries from which these persons come, such consent is almost always given, but it should not be treated as consent sufficient to prevent incrimination for trafficking in human beings for the purpose of sexual exploitation.

The Supreme Court in Switzerland has decided that such a consent given by a person coming from a very poor country will not play an important role. It should be noted that in the case of trafficking, the Protocol to Prevent, Suppress and Punish Trafficking for the purpose of sexual exploitation in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, does not take into account the consent of the person.

In some countries, such as Switzerland, no person may be indicted in a country for a criminal offence which was not committed in that country unless the acts constituting this offence would also be punished in the country where those acts were committed (the "double incrimination problem"). Because of the international dimension of the criminal offences in question in this report, the double incrimination requirement can hinder effective prosecution. A solution would be to grant authority to the government of a country to prosecute its own nationals for acts which constitute a crime under the law of such country regardless of where the acts were committed. The Council of the European Union has adopted a framework decision[2] which would require the member states of the European Union to review all regulations which hinder the incrimination of persons who have committed crimes related to sexual exploitation.

Various programs for the protection of witnesses should on one hand guarantee anonymity to the victims and on the other hand establish the permission for a victim of trafficking to stay in the country in which criminal proceedings are pending during such proceedings so that the victim can testify before the court without fear of deportation.

It might also be useful to consider legislation aimed at regulating matrimonial agencies to avoid the abuse of such agencies in connection with sexual exploitation. One possible direction might be to require strict formal conditions for the conclusion of such a contract. In particular, the conclusion of such a contact over the Internet should not be permitted. A requirement to notify the authorities where the couple will live of the country of origin of the foreign potential spouse or partner might be a useful instrument. In the Netherlands the Supreme Court explicitly stated that the service of arranging fake marriages falls under the scope of the criminal provision of international trafficking in human beings.

Specific proposals concerning Internet

The French legislator's approach towards cybercriminality is worth noting. In accordance with recently introduced legisla-

2. Council Framework Decision of 19 July 2002 on combating trafficking in human beings (2002/629/JHA).

tion, the use of electronic means (i.e. the Internet) in the commission of a crime related to sexual exploitation (trafficking in persons included) is an aggravating circumstance which increases the applicable penalties. This solution is interesting as it avoids introducing new Internet-specific norms.

Contents related to sexual exploitation (mostly child pornography) are often encrypted. To give police the power to order decryption of messages will greatly enhance the ability to prosecute criminals in this domain. In Belgium, for example, a special provision exists that empowers the police to obtain assistance from any expert in the field of encryption.

To make technical intermediaries liable for the illicit contents which they provide would not be a satisfactory solution. A better approach is to foster a constructive dialogue between them and the prosecutors, as well as NGOs dedicated to monitoring illegal contents on the Net. As the examples of Belgium or Switzerland show, these intermediaries are ready to co-operate, especially to block access to illegal websites, on a voluntary basis.

It would be interesting to review regulations in the different national legislations concerning criminal liability of the creator of a hyperlink appearing on an Internet page for the content of the page to which the user is sent via this link, or of the moderators of chats, as these actors can have knowledge about the content of these sites or messages and could eventually provide access to sites related to, or to persons involved in, child pornography or sexual exploitation.

Last but not least, the abovementioned Cybercrime Convention contains a series of powers and procedures, on the domestic as well as on the international level, such as search of computer networks, real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings, interception of data, 24/7 contact points, etc. In order to facilitate the fight against cyber criminality it is of the outmost importance that European states rapidly ratify this convention and implement its provisions. But legal measures are not enough: sufficient resources to finance law enforcement units trained and dedicated to fight cybercrimes are imperative.

B. At international level

There was a need to determine whether the concept of trafficking in human beings for the purpose of sexual exploitation necessarily involved physical movement, or whether attention should also be given to the case of people who did not actually leave the country, or the issue of virtual images. The aim was to update the definition of trafficking for the purpose of sexual exploitation to talk about the transmission of images related to trafficking in human beings for the purpose of sexual exploitation which are detrimental to real persons. In order to do this, the Group referred to the definitions and most recent information contained in internationally approved instruments, namely:

- the Convention on the Elimination of All Forms of Discrimination against Women (Article 6)
- ILO Convention No. 182 on the worst forms of child labour (1999)
- the Protocol to Prevent, Suppress and Punish Trafficking for the purpose of sexual exploitation in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, opened for signature on 14 December 2000
- Recommendation No. R (2000) 11 adopted by the Committee of Ministers of the Council of Europe on 19 May 2000
- the Framework Decision of the European Council No. 2002/629 on combating trafficking for the purpose of sexual exploitation in human beings
- Recommendation Rec (2001) 16 on the protection of children against sexual exploitation adopted by the Committee of Ministers on 31 October 2001 revising Committee of Ministers' Recommendation No. R (91) 11 concerning sexual exploitation, pornography and prostitution of, and trafficking for the purpose of sexual exploitation in, children and young adults.
- the Convention on Cybercrime adopted by the Committee of Ministers on 23 November 2001.

It noted that neither the Council of Europe recommendation on action against trafficking for the purpose of sexual exploitation in human beings, nor the Convention on Cybercrime, nor the additional protocol to the UN Convention against Transnational Organized Crime, designed to prevent, suppress and punish trafficking for the purpose of sexual exploitation in persons, especially women and children, covered the issue of virtual trafficking for the purpose of sexual exploitation. Only the Group of Specialists responsible for revising the Recommendation concerning sexual exploitation, pornography and prostitution of, and trafficking for the purpose of sexual exploitation in, children and young adults[1] had adopted a wider definition of trafficking for the purpose of sexual exploitation, which holds that "pornography" does not necessarily imply the use of a "real" child and that broadcasting images or virtual images is sufficient to constitute pornography as, even though there are no real people involved, the victim is denoted by the image of the person thus depicted (child or woman). *There is no internationally approved instrument on the subject, i.e. the content circulating on the Internet in relation to trafficking in human beings for the purpose of sexual exploitation.*

A short description of each instrument and a list of signatures and ratifications of the relevant international treaties has been drawn up and are attached to this report (Appendices 3 and 4, pages 68 and 69).

1. Recommendation Rec (2001) 16 on the protection of children against sexual exploitation, adopted by the Committee of Ministers on 31 October 2001, revising Committee of Ministers' Recommendation No. R (91) 11 concerning sexual exploitation, pornography and prostitution of, and trafficking for the purpose of sexual exploitation in, children and young adults.

C. Combating the illegal or harmful use of the Internet: how can law intervene? The example of the Yahoo! case

Although the facts had no direct bearing on trafficking in human beings for the purpose of sexual exploitation, the group thought that the legal problems raised by the case and the solutions that were found could contribute to its work. Consequently, it invited Judge Gomez, responsible for the case, to present it, during its meeting in June 2001.

The International League Against Racism and Anti-Semitism (*Ligue internationale contre le racisme et l'antisémitisme – LICRA*) and the Union of Jewish Students in France (*Union des étudiants juifs de France – UEJF*) had observed that Yahoo! Inc. was providing a link to a website that was auctioning objects bearing Nazi insignia. These two organisations had argued that this was an established violation of Article R 645-1 of the French Criminal Code (this article provides that it is prohibited to exhibit Nazi paraphernalia with a view to selling them) and that therefore, whatever the legislation in force in the country from which the website was being run, the fact that these items were accessible to French web surfers was ground for the French judge to take an urgent decision to end this plainly illegal disturbance of the peace. They lodged an urgent application for an interim order against the American firm Yahoo! Inc., which hosted the site concerned, and Yahoo! France for providing a link to the American website from its own website, yahoo.fr.

Judge Gomez had ordered Yahoo to set up a filtering system preventing French web surfers from accessing the American site within three months and to pay a fine of 100000 French francs for each day's delay (see judgment in Appendix 5, p. 72). *This type of action is now dealt with the Convention on Cybercrime, in particular its Protocol on the fight against racism, which aim is to pursue a common criminal policy aimed at the protection of society against cybercrime.*[1]

Judge Gomez also set out the legal problems raised in this case.

1. The European Convention on Cybercrime was opened for signature on 23 November 2001 and its protocol adopted by the Committee of Ministers of the Council of Europe on 7 November 2002.

1. Technical problems

Basically, Yahoo! had argued that it was impossible to filter access to the site 100% in order to exclude French web surfers. However, according to expert evidence supplied, it was possible to make filtering 90% effective. Judge Gomez noted that the following methods could be used to achieve this level of filtering: *geographical identification and filtering by keywords*. The first method was based on identifying IP addresses, which identified each computer linked to the network. According to the experts, 70% of the addresses allocated to French users correspond to French addresses. It was therefore possible to filter them. For the remaining 30%, Yahoo! must ask all surfers accessing the auctions web page and entering a request containing specific keywords (holocaust, Nazi, etc.) to fill in a voluntary declaration of nationality (which supposed good faith). Yahoo! could also rely on the language version of the navigator, which was easy to detect at a distance, and on the destination of the objects to be delivered. Used together, these options constituted a filtering method that was 90% effective.

2. Law applicable

Judge Gomez had to address two questions on this point: *Did French judges have the authority to determine the contents of websites set up in foreign countries? What decision should be taken when the country in which a site was located authorised contents that were prohibited in the receiving country?*

The answer he gave to the first question was that if a site was accessible in France, it fell within the jurisdiction of the French courts. French criminal law was applicable if reception by the user on French territory was an essential ingredient of a criminal offence (in this case, the French Criminal Code considered that it was an offence to exhibit Nazi paraphernalia with a view to selling them). This made it possible to dissociate the site where the offence was actually committed from the site where it produced its effects, giving French courts wide jurisdiction.

The answer he gave to the second question was that there was no question of imposing French law on the rest of the world, or of challenging the legality of the right to make revisionist or racist statements in the United States under cover of the first amendment to the American Constitution, the practical application of which put freedom of expression before the rights of third parties. It was simply a question of technically modifying access to websites in such a way that what was illegal in a given country should not become allowed simply through use of the Internet.

3. Enforcement of the decision

Would an American judge agree to an "exequatur" when the legal basis for Judge Gomez' decision was not recognised under American law? In order for a court decision to be enforced in a foreign country, it must receive an exequatur, a decision conferring authority to execute it. Judgments were only given this authority if the legal basis for the decision was accepted in the justice systems of both countries. This did not apply in the present case, as the United States did not restrict the sale and/or promotion of Nazi insignia, which was illegal under French law.

No answer to this question had been necessary in this case as Yahoo! had decided to exclude Nazi paraphernalia from its auction site. In so doing, it had gone much further than required by the court decision, which was that it should set up a filtering system to prevent French web surfers from accessing the American Yahoo! site.

But it should be noted that in November 2001 a Californian court ruled that *Yahoo!*'s Web site in the USA was subject to US law and thus protected by the First Amendment (which guarantees freedom of expression). *It also rejected the ruling of the French court on grounds of extraterritoriality.*

4. Freedom of expression

The criminal and illegal activities that are growing more widespread on the Internet proved that it is impossible to avoid introducing some form of legal control over this new medium in the name of freedom of expression. The question was what legislation should be adopted to control the Internet and how could it be controlled other than by legislative and regulatory means?

In the framework of this question, the group has discussed the connections between the Yahoo! case and the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation. It agreed that there were undeniably links between the Internet industry, the main new information technology, and trafficking in human beings for the purpose of sexual exploitation ("Mail-order brides"; videoconferencing broadcasting active pornography or sexual violence perpetrated against children; chat rooms, and so on).

The group also agreed that judges could not be expected to control the Internet in particular, and the new information technologies in general, on their own. Preventive measures should first aim at effectively controlling the Internet:

- reform of education and training systems in order to give young people, judges, journalists, teachers, police forces, administrative departments and partners in the private sector tools that would enable them to learn how to use the new technologies and constantly adjust their knowledge to prevent abuse and;
- self-regulation of all the parties involved (authors, service providers, hosts, access providers, transporters, companies and individuals): this entailed raising all the players' awareness of the dangers of broadcasting illegal content on the Internet. It required that codes of good conduct and self-regulating practices should be adopted, and that filtering systems and labelling procedures should be set up;
- the need to strengthen international co-operation: most multilateral instruments were set up within a limited geographical area, confined to Europe. These instruments must reach beyond Europe if the appearance of "virtual havens" was to be prevented.

III. Protecting human rights and guaranteeing the use of new technologies: new challenges

In her report, Ms Hughes stated that internationally, there has been progress in raising awareness and acting against the physical trafficking in human beings for the purpose of sexual exploitation. Unfortunately, the trend has been just the opposite for trafficking in images for the purpose of sexual exploitation. Most people see the reduction or elimination of prosecution of adult pornography as being a victory for the individual rights of people and an end to suppressive government enforcement of morality based laws. The challenge is to change attitudes, policies and laws that connect the acts and images in ways that preserve rights of freedom of expression, but protect the rights of human beings to be free of criminal acts of trafficking for the purpose of sexual exploitation.

The group decided to examine these new challenges involved in protecting human rights and guaranteeing proper use of new technologies, in particular the effects of the use of new information technologies on the victims of trafficking for the purpose of sexual exploitation, freedom of expression and the Internet and the role of the media.

Through the information gleaned from the questionnaire replies, to which were added details of new cases, involving both children and adults, communicated by members of the Group, examples of action against trafficking in human beings for the purpose of sexual exploitation via new information technologies appear to be more common in the field of child pornography than in cases involving the exploitation of adult pornography or the exploitation of prostitution.

In most of the countries which replied to the questionnaire, there are national structures capable of ensuring co-ordination of the fight against the harmful use of NITs in relation to sexual exploitation and trafficking in human beings, for the purpose of sexual exploitation Usually these are police department, or different departments in the Ministries of the Interior or other bodies or organisations linked to the use of Internet. In some countries, a co-operation was set up between the representative organisations and the courts or the police.[1]

There are also three organisations at the European level: EuroISPA which brings together Internet service providers from member states;[2] INHOPE (the European Association of Internet hotline providers), and INCORE, a project to set up a system for describing web-site content, which, like INHOPE, is funded by the European Commission under its Action Plan to Promote Safer Use of the Internet. [3]

At international level, this role is played by UNICEF, INTERPOL, the Association "Innocence in Danger".

Little information was provided on cases of the harmful use of new technologies in relation to pornography, sexual exploitation or trafficking for the purpose of sexual exploitation. Twenty of the forty-three member states of the Council of Europe replied that they were not aware of any such use and only seven countries gave concrete examples However, cases constitute an important element of the study of this issue as they give an overview of the phenomenon, they provide information on the victims and the users and on the way the latter operate.

There are more examples of child pornography related to the use of NITs than on adult pornography. For instance, Inspector Paul Holmes of the Metropolitan police describes the case of the dismantling of a Lithuanian computer network controlled by a British citizen and which used Internet to provide the services of Lithuanian prostitutes in London. Ms Linda Regan (London University) also reported a case of women filmed while being abused and the films were then broadcast on the Internet. The representative of the Association Reden (Denmark) refers to a case of seven South African women available on Internet as Indian women. A member of the Animus Association (Bulgaria) related the case of a woman blackmailed by her former partner who threatened to use her photos on Internet. In Portugal, in 1998, the Ministry of Culture ordered that a site be closed after the discovery of a page including pornographic images drawn from a comic cartoon series. In Latvia, a company[4] operating as a fashion agency produced and published on Internet pornographic images and films as well as advertisements for sexual tourism.

As far as child pornography is concerned, cases involving several persons were reported. They are often international net-

1. See document EG-S-NT (2001) 8.

2. Austria, Belgium, Denmark, Germany, Spain, France, Ireland, Italy, the Netherlands, Sweden, Finland and the United Kingdom.
3. See document EG-S-NT (2001) 10.
4. This case was also described by Ms Hughes in her study on the users.

works perfectly organised and operating in a professional way (entry code, coded language, etc.). For example: Operation "Cathedral" (September 1998) in which approximately one hundred persons belonging to a pedocriminal club were arrested in twelve countries in an operation co-ordinated by the British police with the active participation of police services from other countries and Interpol, or the Affair "Lolita-Club" in 1997.[1]

Also, in Russia in 2000, the Ministry of the Interior received information from Germany, Sweden and Austria on the involvement of Russian citizens in the distribution through Internet of paedo-pornographic material. A group of suspects was arrested in Rostov.

Cases of persons acting individually from their own sites were also reported: in Finland, the case of a student using two computers to distribute images of a sadistic nature with Caucasian and Asian children. In Germany, the case of a doctor from Berlin condemned to two years of detention for the distribution of paedo-pornographic material on Internet; or a case of a schoolboy in Pforzheim who used his computer to distribute child pornography images on Internet.

There were also cases of persons using a legal entity which already exists (university, trade company, etc.). For example, in Poland, in 1996, a company used legally an Internet site and decided, to pursue its development, to create another independent server. A computer specialist working for the company took advantage of his position and created two personal sites without the agreement of the management in order to distribute paedo-pornographic material. There were also cases of persons acting under the cover of a legal entity created specifically for this purpose with a legally recognised objective: in Hungary, a person was condemned for having created a centre for fashion photography in a small Hungarian town and for having used photo sessions to produce pornographic material with the participation of children and diffusing it on Internet. There also was a similar case in Latvia, but it concerns a much larger company also active in the field of adult pornography and prostitution.

It should be recalled that the low prices of computer material and the attractive deals which make it possible to "surf" the Web partly explain the increasing use made of Internet by paedo-criminals (see, for example, the statistics shown in a table giving the number of denunciations recorded by the Swiss local police concerning article 197 of the Penal Code (hard pornography) in relation to Internet from 1997 to 2000).[2]

The images available are more and more obscene, perverse and brutal and pedocriminals do not hesitate to use young children, including babies. In order to be able to intervene effectively against this form of criminality, the police need a perfect command of computer techniques. In addition, networks can be neutralised only by action coordinated at international level.

Most of the countries which replied to the questionnaire considered that the national bodies competent in the field co-operated with bodies of other countries. The international organisations most often mentioned were INTERPOL and EUROPOL.

NGOs from different countries also work together (for example "La Strada", Poland – "La Strada", Ukraine). At international level, exchanges of information also take place in the context of the Vienna Conference on child pornography or ECPAT (End Child Prostitution in Asian Tourism), which is an NGO network in 50 countries for the elimination of prostitution, pornography and trafficking for the purpose of sexual exploitation of children

According to the replies given to the questionnaire, the present system shows strengths and weaknesses. The closer co-operation between the bodies in charge of fighting computer criminality related to sexual exploitation (exchanges of information and experiences between police departments of different countries, between police departments and Interpol, between police departments and NGOs, between NGOs) was considered as a strength. But the national legislation in force and the procedures set up and the systems for exchanging information are considered as weaknesses. In most countries, the technical means used are far too slow compared to the speed of the new technologies and to the phenomenon in question.

Mr Walraet, from the Federal Computer Crime Unit (Belgium) was asked by the group to present the techniques used by law enforcement to fight harmful acts on Internet and the problems encountered. His study is presented below, and is completed by a case study.

1. This case is described by Mr Walraet in the chapter "Law enforcement and cases" of this report, below.

2. See document EG-S-NT (2001) 7.

A. Law enforcement and cases

New inventions and in particular the very rapid growth of computer technology have given a new dimension to the problem of the sexual exploitation of human beings or the dissemination of pornographic or pedocriminal photographs and texts.

"Bulletin Board Systems" and the Internet have made it much easier to disseminate this kind of material. Everyone anywhere in the world can send or obtain pornography at an incredible speed, virtually anonymously, without leaving the home.

The Internet is without question a medium which offers unprecedented advantages: it is a vast, living, inexpensive library which can be consulted by anyone the world over. The Web is a cultural, economic and social improvement. Unfortunately, unscrupulous persons use the Internet for dishonest purposes. Pedocriminals, pornographers, sects and others have been quick to realise its enormous potential. As the Internet is a medium virtually without mediators or borders, illegal or harmful acts committed on it entail less risk.

Trafficking in human beings for the purpose of sexual exploitation under the cover of offers of employment or e-mail based marriage agencies, sex tourism, trafficking in children for the purpose of sexual exploitation through so-called adoption agencies, the sale of pornographic photographs and texts, real time "video conference" or telephone pornography and catalogues of prostitutes are just a few examples of phenomena which have grown enormously thanks to the Internet.

1. Legislation

The first question which should be posed is whether the current legal system provides the necessary laws for dealing with the problem.

Most countries have legislation under which the authors, distributors and peddlers of child pornography may be prosecuted, trafficking in human beings for the purpose of sexual exploitation and the exploitation of prostitution can be fought, even when such offences are committed through the medium of the Internet. But for other phenomena, even if they are very harmful, the legal means available are not always sufficient.

Clearly, in democratic countries the fundamental right to the free communication of thoughts and opinions and the right to secrecy of correspondence are intangible, but all too often, criminals misuse these rights to disguise the real nature of their activities.

The production of pornography, marriage agencies or advertisements for prostitutes may conceal an organisation that exploits women or children sexually, using threats or violence to force them to submit to what are sometimes inhuman acts.

The authorities and the police will always find it difficult to distinguish between these cases, and the fact that this takes place on the Internet certainly does not make matters easier for them. Hence the need to give investigators more technical and financial resources and provide sound training on the subject.

Even at national level it is no easy matter to deal with criminals who use the Internet, and it is all the more difficult if they are operating from abroad. Sentences may be passed in certain cases, but are rarely enforced in the countries in which such persons are active. Also, most countries are unwilling to allow an application for extradition if it concerns one of their citizens.

In most cases, the sole means open to the police is to send the incriminating evidence to their counterparts in another country via the usual Interpol or Europol channels. If the laws of that country permit, and if the actions are punishable, the perpetrator may be prosecuted.

This is very time-consuming, but currently, owing to the international nature of the Internet, it is usually the only solution. In any case, if offences committed via the Internet are to be combated, carefully drafted international agreements on procedures, court and police co-operation and law enforcement are needed.

2. Problems which need to be solved

It has always been difficult for the police to cope with the problem of sexual exploitation. The world of pornography and of exploitation of prostitution is very closed, sexual abuse and trafficking in human beings for the purpose of sexual exploitation is often not discovered unless the victims dare to speak out, or else by accident.

With the Internet, even if it has made the material in circulation more visible and accessible, things have begun to change: like it or not, criminals communicating on the information highway or using it to ply their "trade" must reveal their identity from time to time. It is possible to monitor, at least in part, what is happening on the Internet and to uncover offences with the help of thorough controls. That way, criminals can be traced, offenders arrested and misdeeds prevented.

3. How the Internet is used

Electronic mail (e-mail) is used to send messages and files of all kinds to anyone with Internet access anywhere in the world. E-mail is personal and covered by the secrecy of correspondence and communications, which is why it is often employed by criminals to send photographs or messages. These individuals sometimes utilise this means of communication to send junk mail or "spam" to Internet users who have never requested it. In so doing, they hope to find customers for their activities.

An electronic monitoring of the content of the electronic messages sent is virtually impossible and is also illegal in many countries In general, the content of electronic messages is only acceptable as evidence if it was discovered during a house search or was communicated to the authorities by the addressee. *But it should be noted that a recent decision (2002) was taken in the UK by Lord Woolf, the Lord Chief Justice, which ruled that Internet service providers can lawfully intercept e-mails at the request of the police once they have received notification that a special production order is being sought from the courts.*

Newsgroups include not only pedocriminal ones containing child pornography, but also ones which contain data on brothels, women (or children) who "work" there, prices, experiences, what to do to circumvent police checks, contact persons etc. Unlike e-mail, these newsgroups can be monitored. Their content is present on Usenet servers, an integral part of the Internet, and is universally accessible, and the messages can be read and downloaded.

Message headers sometimes contain information making it possible to identify the sender by means of logfiles kept by the access provider.

Since the creation in 1992 of "Computer Crime Units" by the Belgian police, newsgroups with pornographic and above all pedocriminal content have been regularly monitored. This has already led to the identification and arrest of a number of pedocriminals and other sexual offenders. In certain cases, e-mail and messages from newsgroups have been secured while examining the content of disks, thereby allowing the investigation to be pursued and other implicated persons to be identified.

Monitoring the content of pornographic newsgroups is very time-consuming. Anyone who is familiar with the Web knows that some of these newsgroups contain dozens or even hundreds of new messages every day. Reviewing them manually becomes an endless undertaking.

As the header of the message sent indicates its source, some users employ anonymous remailers, not only for messages in newsgroups, but also for e-mail. These computers remove data from the header which reveal the source of the message before it is sent to its true destination, thus making it impossible to know where it originated. The anonymous remailer stores in its database an identification of the message sent as well as the

real electronic address of the sender, to whom any replies can then be directed.

The only way to retrace the origin of such messages is to be able to access the anonymous remailer's database. Since these machines are often located abroad, the police depend on the good will of the operators of these systems for the communication of necessary information.

Another solution is to send requests for judicial assistance to the authorities of the countries in which these machines are located. As this takes considerable time, the information requested may have already been deleted before the request is approved.

The only solution, according to Mr Walraet, is to pass legislation making anonymous remailers illegal or requiring them to retain information making it possible to identify the authors of messages for communication to the authorities upon requisition by a judge in the context of a court inquiry. But this can only work if all countries from which the Internet can be accessed take the same decision.

Such measures will be regarded by some as an invasion of privacy or a violation of the secrecy of correspondence, but Mr Walraet is convinced that these fundamental rights must not be misused to ensure impunity for individuals who care little about the rights of their fellow citizens.

Another problem with which the police authorities must increasingly contend is that messages are ciphered, making them impossible to read. A number of solutions have already been proposed, ranging from legislation prohibiting encrypting by individuals to a databank containing encrypting keys. But, according to Ms Hughes' study, several law enforcement officials in the UK and the US indicated that at this point the capabilities and threat of encryption seemed to be talked about more than it is used. Encryption programs are not easy to use, and other methods of hiding activity or content are more popular.

Each method has advantages and drawbacks, but, given the enormous sums of money involved, any punishment which may be imposed in response to a violation of legislation or utilisation of a non-registered key will not deter criminal organisations. In Mr Walraet's opinion, the only solution to the problem is to try to have specialised laboratories develop decrypting programmes and high-performance computers. Clearly, these laboratories will need budget funding, although 100% results cannot be guaranteed, at least not in the beginning.

Turning now to Web site monitoring, a number of these sites offer free access to some of their pages, but require a subscription to access the more hard-core material. So it is very difficult to know what the exact content is of a site under surveillance. Some sites merely offer to sell erotic CD-ROMs, books, catalogues or holidays, but do not give many details on the products sold. For this reason, the only way to learn about criminal offences is if subscribers are annoyed by the material or information and report what they know to the police authorities.

Consequently, in 1996 the Belgian police created a Web site (http://www.gpj.be) with a "child pornography hot-line" in order to offer all Internet users the possibility of anonymously providing information on offences relating to child pornography. All usable information is processed by the Belgian services or forwarded to the responsible foreign authorities.

In view of its success, the Belgian police has broadened the "child pornography hot-line" in a general hot-line through which it would be possible to communicate all information about illegal, harmful or offensive content: trafficking in human beings for the purpose of sexual exploitation, fraud, etc. Experience has shown that many people have very useful or revealing information but are afraid to pass it on directly to the police. This hot-line would make it easier for them to do so.

It should be noted that many countries replied to the questionnaire that in order to gather information on illegal material available on Internet or on crimes committed through NITs, they also created "hotlines". For example:

- Austria - hotline ISPA and hotline on child pornography
- Denmark - hotline of the "Save the Children" association
- Germany - 3 hotlines on child pornography
- Netherlands - hotline Meldpunt against child pornography
- Sweden - Radda Barnen hotline
- France - AFA contact point on child pornography
- Moldova - hotline of the Centre for the prevention of trafficking in human beings for the purpose of sexual exploitation
- United Kingdom - hotline of the Internet Watch Foundation aiming to detect any illegal content on Internet
- Finland – web pages of the "Save the Children" association
- Interpol European working party on information crime.

Web pages and e-mail addresses have also been made available to the public by the police. Information may also be sent to police departments or other bodies regulating the Internet.[1]

The last aspect of the Internet, and not the less important, concerns "Internet Relay Chat" (IRC) and the ICQ. These real-time multi-user conversation systems, which are perhaps less well known to the average Internet user, are frequently employed to exchange (child) pornography, set up FTP servers linked to the Internet or hold "video-conference" sessions. Specialists claim that most child pornography transits through this medium. Ms Hughes explained in her study that there have been numerous cases in the United States and the United Kingdom of predators contacting children for online and physical meetings in which children have been emotionally and sexually abused. There have been numerous cases of online stalking of adults that began with conversations in chat rooms, and led physical meetings that turned into sexual assaults.

Unlike messages sent via newsgroups, IRC conversations do not leave any trace. Files sent or exchanged during communications sessions are not saved anywhere on the Internet; they are sent in real time directly to their addressees. For the police, the only way of responding to everything happening on certain IRC channels is to be present while the conversations are going on and to try to identify the individuals violating the law.

One major problem is that in many countries entrapment is illegal. Even if the police are present during a conversation, they must be very cautious. In some countries, certain forms of entrapment are legal. For example, it is more likely that a pedocriminal looking for sexual contact will make a proposition to someone who pretends to be a ten-year-old girl than a bald 40-year-old man with a beard. In certain countries, for example the United States, a pedocriminal may be arrested as soon as he takes steps to arrange a meeting with a child for the purpose of sexual abuse or exploitation.

1. See document EG-S-NT (2001) 9.

Some people disagree with the use of such methods. But if a pedocriminal makes a proposal to a policeman pretending to be a child, he would do the same with a real minor. Mr Walraet is convinced that in the case of child pornography, and trafficking in human beings for the purpose of sexual exploitation in general, this constitutes a good working method for combating sexual abuse, one which the police should be allowed to use in all countries.

Pornography, and with it the sexual exploitation and trafficking in human beings for the purpose of sexual exploitation, has become a real industry. In the United States for example, it generates an annual turnover of ten billion dollars.

As the Internet is an inexpensive and readily accessible medium, some use it like a real mail-order company, not only for peddling pornographic material but for actually selling human beings. The Internet has real world-wide catalogues and guides on red-light districts and brothels, so-called marriage bureaux, sex tourism agencies etc. It is thus clear that many people will defend their lucrative trade and will make the work of the police authorities as difficult as possible. There is still a long way to go, and it is a never-ending battle.

The Internet is relatively new in many countries, and so appropriate procedures and legislation are still needed. Every country should be able to have applicable legislation concerning the Internet which makes it possible to root out sexual exploitation. But in view of the international nature of the Internet and other means of communication, national legislation alone is not enough. Really attacking the problem calls for carefully drafted and standardised international procedures, including minimum rules. Here are a few suggestions:

- Good police training on using the Internet is needed, as well as good international procedures and agreements between national police authorities. Communicating via the Internet is so easy and works so fast that certain current procedures are no longer applicable. Sometimes it has to be possible to intervene immediately, without losing a single minute.
- Agreements between the authorities and Internet service providers must be further improved; this concerns the communication of information on illegal data on the network.
- Legislation must be passed defining minimum data to be kept accessible for the authorities by access and service providers so that the source of material sent by the Internet can be identified. Such legislation should also stipulate how long these data must be saved.
- A solution must be found for problems of encrypting and anonymous remailers.
- In the future, the content of the Internet as well as all new technical developments used must be closely monitored; this can be done by setting up hot-lines.
- A solution must be found for data sent from "Internet havens", countries for prosecuting certain types of crime.
- In many countries, legislators and decision-makers are often oblivious to what really is happening on the Internet and must be made aware of the issues involved.

It should, however, be borne in mind that the Internet does not operate in a legal vacuum, as many seem to think. Every person involved may be held accountable for his acts. But it all depends on how the problem is tackled in the future.

4. Retention of vital communication traffic data by telecommunication operators and telecommunication access and service providers

Taking into consideration that communication networks – including the Internet – are frequently used to commit crimes, law-enforcement authorities need to be able to use traffic data[1] for investigation and prosecution purposes.

By using the traffic data stored or used by telecommunication operators, communication access and service providers,[2] it should be possible to trace back and locate geographically and chronologically the end-user device[3] that was used to commit the crimes (i.e. to transmit the information or to operate or manipulate a system from a distance).

Communication technologies can be used to :

- transmit any kind of data
- control and operate from a distance computer and telecommunication systems, machinery and equipment.

1. Information elements on the signal/data transmission needed to realise or to control the telecommunication; **does not include** the contents of the communication.
2. Internet Access Providers are companies that provide access to the Internet, generally through dial-up access (modems), cable modems or wireless connections. IAPs and ISPs (Internet Service Providers) are often used interchangeably. IAPs can be considered to be a subset of ISPs, who provide additional services (leased lines, developing and/or hosting web sites etc.). Online Services provide their clients with data and with an infrastructure that permits communication between the subscribers (mail, conferences, forums, etc.).
3. The device (computer, telephone ...) used by the final user (the client).

5. Why must traffic data be preserved?

1. *Because of the fact that the acting person is physically not present at the place of the real impact of the action, and therefore no physical traces can be found, telecommunication trails are the only way to investigate the crimes.*

   Erasing or not keeping those trails would have the same effect as e.g. wiping fingerprints or blood stains at a murder scene.

2. *Anyone can connect to and communicate through telecommunication networks, very anonymously, from anywhere in the world. The use of aliases and nicknames makes the user information and identity data unreliable:*
   - false or non-existing E-mail addresses can be used[4]
   - identity or subscriber data communicated to providers is in many cases (e.g. free access and/or e-mail providers,[5]

4. In most applications (mail, newsgroup, chat programs, etc.), the user can put a false or non-existent e-mail address during the configuration of the application; when an e-mail, news message, etc., is sent, the false or non-existent e-mail address will then appear as the address of the sender, which makes it unusable for his identification.
5. Companies that offer free Web space or free E-mail addresses.

free Web space providers) not checked by that provider; thus free e-mail addresses, log-ins, Web space,[1] etc., can be obtained without communicating real identity information

- a number of open communication and data transmission channels (chat rooms,[2] peer-to-peer networks,[3] newsgroups,[4] etc.) do not require the communication of, or do not show, any identity data
- most of the free access providers do not control – and in most cases do not have the means[5] to control – the identity or subscriber information communicated by their users; on the other hand, they are able to log the communication data that can be used to trace the client.

3. *Content data (contents of E-mail messages, web pages, ftp-files, etc.) often do not contain any information that can lead to the identification of the sender or creator of the files (use of anonymous remailers,[6] e-mail addresses obtained with false subscriber data, etc.)*
4. *Transaction data (data about selling/ordering goods and/or services, etc.) or payment data sometimes do not contain the necessary elements to identify the author of the crime (think e.g. of a perpetrator using a false or stolen credit card number to get access to data).*

Only telecommunication traffic data is left for investigation purposes, because it is often the only data that cannot be tampered with by the perpetrator. Without these data, it is impossible to investigate or collect any other reliable evidence.

1. Free Web space (a number of megabytes) can be obtained on the Internet, in which it is possible to put information, images, video files, etc., that can be accessed by anyone who has an Internet connection.
2. An Internet channel (virtual room) through which people can communicate in real time using a computer; some chat programs also offer the possibility to exchange data (text files, images, etc.) and/or to have a private chat session between two (or more) persons (if they are admitted).
3. Peer-to-peer is a communications model in which each party has the same capabilities and either party can initiate a communication session. In recent usage, peer-to-peer software is used to permit people to exchange files with each other directly or through a mediating server, using the Internet. The user must first download and execute a peer-to-peer networking program (e.g. Kazaa, Bearshare, Morpheus) that allows him to exchange all types of files. After launching the program, the user can connect to another computer connected to the network. Normally, the web page where the user got the download of his program will list several IP addresses as places to begin.
4. Forums, or on-line discussion groups. On the Internet, there are thousands of newsgroups covering every conceivable interest (also child pornography, prostitution, drugs, etc!!!). To *view* and *post* messages to a newsgroup, you need a "news client program" (e.g. Microsoft Outlook Express, Netscape Navigator), a program that runs on your computer and connects you to a news server on the Internet, where the messages can be read and posted.
5. Private companies don't have access to (government) databases that contain the identities and addresses of people; because the web space or other services are free, there is no payment data neither.
6. A privacy service (Web site) that is set up to allow users to post their e-mail or news message without leaving any trace; the anonymous remailer strips off all data in the header of the message that could lead to the identification of the sender. The remote server (where the mail or news message is sent to) receives information about the anonymiser server, in place of information about the sender's computer. The information in the header is in most cases replaced by a code that allows the anonymous remailer to forward possible replies to the sender of the original message.

6. Why is real-time or expedited traffic data collection not enough?

Several crimes are discovered only after several weeks or even months, when the crime has already stopped; trying to collect information from the moment on of the discovery would in those cases lead to nothing.

Real-time collection starting at the moment the crime is discovered, even if it is discovered immediately, makes it impossible to investigate crimes that are only committed once or that are not repeatedly committed through the same channel.

In ICT[7] crime and abuse of ICT-systems for criminal purposes, perpetrators (who have in most cases a lot of knowledge) seek not to be detected, in order to be able to continue to use the same channel. In most of the cases they succeed in doing so. When the crime is at last detected (sometimes after several months), expedited preservation will in most cases be in vain (think of the free or flat rate telecommunication services that don't need traffic data for billing purposes)

Vital traffic data

Without the vital traffic data, no cyber investigation can be started or continued to the end.

The following data have to be considered as vital:

1. Data in relation to the connection to the data/signal carrier (e.g. fixed-line telephony, GSM, cable connection, satellite telephony):

- called number
- calling number
- intermediate numbers (call forwarding, conference calls)
- date and time of start and end of communication (or start and duration)
- type of communication (incoming, outgoing, forwarded, conference ...)
- geographical location of the connection of the end-user device to the telecom network
- identification numbers of the end-user device (telephone number, MAC-address,[8] modem serial number ...)

2. Data in relation to the connection to the data network:

- Level 1 protocol subscriber identification (e.g. IMSI,[9] MSISDN,[10] modem serial number ...)

7. Information and Communication Technology.
8. On a network, the MAC (Media Access Control) address is your computer's unique hardware number. When you're connected to the Internet from your computer, a correspondence table relates your IP address to your computer's physical (MAC) address on the network.
9. International Mobile Subscriber Identifier, a 15-digit number used within mobile phones that allows service operators to identify mobile terminals, for purposes of international roaming.
10. Mobile Station ISDN Number, a dialable number, a 10-digit NANP (North American Numbering Plan) directory number assigned to address a wireless service subscriber.

- Network user address (e.g. IP address[1] of end-user for Internet connection
- dynamic or fixed
- details of used user accounts, leading to the name and address of the user)
- date and time of start and end of communication (or start and duration) for Internet connection: from which telephone number the connection was made, or the physical address of the system(s) used.

Because of the quick evolution of the technologies and services, it is impossible to give a complete and definitive list of the vital data that should be preserved for investigation purposes.

Retention period

Making rules for the preservation of communication data must not only be based on the need of solving crimes related to trafficking for the purpose of sexual exploitation of human beings, traditional or organised crime, but must also take in consideration other forms of crime where new technologies are used. Especially where ICT-crime (hacking,[2] illegal copying of information, sabotage) is involved (or used to commit other crimes), a longer retention period is certainly necessary.

One must take into consideration:

- "preparation period" during which ICT systems are searched for vulnerabilities, communication lines and –systems are set up, accounts are prepared, etc. The prepared systems are, in well-organised crime, not used immediately but in some cases only after several months
- the period between the actual crime and the moment it is discovered
- the time it sometimes takes for a victim to decide to file a complaint or to tell what happened (e.g. trafficking for the purpose of sexual exploitation in human beings, child pornography ...)
- the time it takes before the case is brought to the specialised police force
- the fact that sometimes several intermediate systems ("stepping stones")[3] are used, different countries; in those cases, the result of one country must be obtained before an official request can be sent to the next country, and so on. Besides the sending of letters rogatory often takes quite some time.
- the differences of the legislation in different countries, which may cause delay.

1. A 32-bit number (in the Internet Protocol Version 4 definition; 128-bit in version 6) that identifies each sender or receiver of information that is sent across the Internet. When connecting to the Internet, your computer is assigned a unique IP address out of a list of addresses that belong to your provider. The IP address, in the case of a dynamic IP, is assigned to your computer for the duration of your active connection to the Internet. When your connection is ended, the IP address can be assigned to another user's computer. In the case of a fixed IP, your computer has the same address during every one of your connections to the Internet.
2. Breaking into a system, with the purpose of stealing, deleting or altering information, taking over or using the system, etc.
3. E.g. a hacker can break into a system in one country, from that system break into another system in a second country and so on, to finally arrive in the victim's system. When trying to identify the hacker, the trace must be followed in reverse order. Only when the results have been obtained from the authorities of the last country in the chain, information can be requested from the authorities of the following country and so on.

Reference can be made to the report of the "Interpol European Working Party on Information Technology Crime",[4] which, after a long and in-depth study of several cases, came to the conclusion that, as it is not possible to make the distinction between telecommunications during which cybercrimes are being committed (or cybersystems are used to commit crimes) and normal communication use, the retention period for vital traffic data should be set to no less than 12 months.

Mr Walraet illustrated his report on law enforcement and cases by the description of a case "Operation 'Too Young'", exchange of child pornography through the Internet.

❖ "Operation 'Too Young'", a case of exchange of child pornography through the Internet

In May 1997, the Computer Crime Unit of the former Belgian Judicial Police discovered a message in a Japanese newsgroup. A person using the alias "Chico" was looking for members for what he called the "Lolita-Club". The aim of the club was the exchange of child pornography through the Internet.

In his message, the person mentioned a valid e-mail address. Therefore his access provider was requested by the Magistrate to reveal his identity for investigation purposes. But the information we received turned out to be false.

Normally a new client had to fill in a form for the access provider, who then sent the log-in and password to the address mentioned on the form. In this case however, the individual went to the access provider himself and asked to obtain the log-in and password immediately, telling he needed it as an anniversary gift for his nephew ("social engineering").

Because of the false information, another way to identify "Chico" had to be found.

So the access provider was requested to hand over the logfile information of the client's Internet account (logfiles containing date, start time and duration of the Internet access).This information showed that he had always accessed the Internet through the same POP (=point of presence) of the provider, more precisely through a telephone line.

However, the logfiles didn't mention the calling number and the provider didn't have at his disposal the technical means to log this information during later log-ins. Moreover, "Chico" was not using his account at that time of the investigation. For that reason, the national telephone company was requested by the Magistrate to hand over the incoming calls logfiles of all the telephone numbers of the access provider's POP, used by the perpetrator (75 lines).

By comparing the access provider's logfiles and the ones of the telephone company, the perpetrator could finally be identified.

It is obvious that it would have been impossible to identify "Chico" without the above-mentioned logfiles. A warrant was issued by the Magistrate for the seizure of the perpetrator's e-mail. This mail contained only the text and the attached files of the incoming e-mail. For what outgoing mail was concerned, the provider could only log the destination E-mail addresses, not the contents of the messages.

4. See Appendices 6 and 7, pages 80 and 82, Scheme of the conceptual approach to determine the traffic data to retain, Catalogue of traffic data (version 27/11/2001). Sources: "Expert statement of the Interpol European Working Party on Information Technology Crime".

The analysis of the received mail showed that Chico was the organiser.

To become a member of the club, three child pornography files had to be sent to him. Then he would communicate the e-mail address list of the other members. The new member had to send 2Mb of child pornography files (and afterwards 500Kb per month) to all other members.

A list of the files already sent was kept by "Chico".

Further analysis showed that persons in fifteen different countries were involved.

A CD-ROM was made by the Belgian police force, containing a summary table and all available information (e-mail address, aliases, sent files, etc.) per country and per club member. It was, at the request of the Prosecutor, sent to Interpol and from there to all the countries involved. With the help of Interpol, an international operation was set up under the control of the National Magistrate. International co-ordination was necessary because of the different legislations in different countries, the danger of leaks and thus the disappearance of evidence (Internet = speed!).

On 26 November 1997 perpetrators in twelve different countries were interpellated simultaneously. The results were positive in all participating countries and different arrests were made. An immense number of image files, videotapes (also "home made"), scanners, CD-writers, cameras, etc., were seized. Some of the perpetrators confessed child abuse, in some cases of their own children.

Even though in the end the organiser of the club, Chico, did not turn out to be a real child abuser, identifying and investigating him lead police forces to real child molesters all over the world.

If connection information had not been logged, finding out about those child abusers would not have been possible, or at least some of them would have escaped or been arrested much later.

B. The effects on the use of new information technologies on the victims – Protection of the victims

1. Different types of victims

Prevention of trafficking in human beings for sexual exploitation is a problem that public authorities across Europe have to address.

The use of new information technologies for trafficking in human beings for the purpose of sexual exploitation *creates different kinds of victims*. The Internet is used by traffickers to "recruit" potential victims. Ms Hughes noted in her study on mail bride orders that the women most vulnerable to recruitment were young women, aged 19 to 22, living in extreme poverty, in regions where unemployment is high and the prospects for the future are poor. There are also victims of domestic violence, whose images are circulating on the Internet. The Group also identified other examples of victims. It discovered, in particular in the study made by Ms Hughes, that a number of users were involuntary users, often minors, in some cases lured into the business through harmful use of technologies by traffickers, and that these users were themselves potential victims.

During the workshop on "good" and "bad" practices regarding the image of women in the media, held in Strasbourg in 1998, Ms Monika Gerstendörfer,[1] psychologist and member of the Group of Specialists, described the various kinds of victims and completed this list in her contribution to this report. They are:

- women and children who are directly abused through the production of videos
- children and women abused/tortured for the purpose of pornographic productions (pictures, videos, interactive CD-ROMs)
- children and women from poor countries and/or countries in war
- surfing children who get into contact with interactive porn or videos
- surfing children who get into contact with and/or are being "groomed" by pedocriminals in the Internet Relay Chat
- children "made" perpetrators by pedocriminals or others by abusive use of interactive "games" on CD-ROM
- children whose behaviour is strongly influenced by the content on the Internet, they are forming their opinions and attitudes about sexuality, about norms and acceptable practices
- persons who survived porn productions retraumatised because of the new possibilities of the IRC, the WWW and other IT tools
- re-traumatised young adults and adults who survived such "productions" in their childhood or youth, but have knowledge about the possibilities via IT to prolong their suffering (distribution of their pictures, etc.)
- some victims of porn productions who dare to speak in public about their torture and are threatened by perpetrators
- parents of victims who can find photos of their children when using the Internet.

She also added to the list the policemen, researchers and the NGOs experts who are confronted daily to violent cases and can be considered as indirect victims, as they did not get the necessary support or help in their work. The impact of images on policemen, researchers and NGOs members and the support – financial, social or psychological – they need to continue their work should be taken into account.

1. Monika Gerstendörfer, psychologist, *Lobby für Menschenrechte* (lobby for human rights, NGO) Metzingen, Germany.

2. The effects on the use of new information technologies on the victims

As regards *the effects on the use of new information technologies on the victims*, the images available are more and more obscene, perverse and brutal. Pedocriminals do not hesitate to use young children, including babies.

Fundamental human rights such as the right to life, the right not to be subjected to torture or to inhuman or degrading treatment are threatened by violence or trafficking for the purpose of sexual exploitation used to produce images broadcasted on Internet.

An NGO in Denmark working with victims of prostitution, pornography, and trafficking for the purpose of sexual exploitation described the harm done to women. They say that the new capabilities of the Internet further the harm to victims:

> "Contact with victims of prostitution, porn and trafficking for the purpose of sexual exploitation has given us information on the long-term harms done to people having been projected on the Internet. Pictures and video films never grow old and can be found on the Internet many years after the actual person has stopped acting in this business, which is seriously violating the person involved. The psychological damage done to victims in this ways is very harmful. You can find pictures 20-30 years old while surfing the web, also images of children being abused. Adults can in that way find pictures of themselves being sexually abused as children many years after the abuse has stopped. And they have no possibility to get these images removed from the Internet, even when they know where they are shown."[1]

Women and children are hurt physically, sexually and psychologically. They can contract sexually transmitted and other infectious diseases, such as tuberculosis. They suffer from post-traumatic stress, depression and anxiety. They often use drugs and alcohol to numb themselves, and attempts of suicide are common.

The effects are also linked with *racism*, in that trafficking for the purpose of sexual exploitation in human beings is often related to immigration issues. According to some research, it seems that more images are made of children from Eastern Europe, in particular younger girls:

> "Through the analysis of its database of child pornography, the COPINE Project found that the majority of children used in the making of pornography are white, with fewer being Asian, and almost none being black. The analysis of images on child pornography newsgroups indicates that the average age of the children, especially the girls, is getting younger, and more images are being made of children from Eastern Europe."[2]

Forced prostitution and trafficking for the purpose of sexual exploitation also restrict women's freedom and fundamental rights. This is linked to the issue of violence against women and equality between women and men. Ms Hughes mentioned in her report that the pervasiveness of pornography in the workplace through Internet access, raises concern for women's equality in the workplace. How are women likely to be viewed and treated if their male colleagues are engaging in so much work time using pornography. People's, especially teens', attitudes toward women and men, their expected behaviours, roles and rights, are being strongly influenced by the content on the Internet. Considering the misogynistic content of much of the material, it does not bode well for equality between women and men.

1. Reden, International Abolitionist Federation, Denmark, Spring 2001.

2. See the study of Ms Hughes on the users.

3. Different types of perpetrators

For Ms Gerstendörfer, it is also very important to understand the variety of motivations of the perpetrators in order to get aware of the different dangers for real and future victims. What are the motivations of the different groups of criminals? Organised crime has a central position in this field, but there are other kinds of perpetrators. To know them could help in many aspects (laws, kind of punishment, sense of therapies, etc.).

As regards the *consumers* of pornography, researchers at the COPINE Project in Ireland made the following observation about the lack of information about consumers of pornography. In this case, the authors were referring to child pornography collectors:

> "A major weakness in contemporary work in this area is that it does not consider how individual consumers use and understand pornographic or other photographic media nor does it acknowledge their choice, responsibility and accountability for their behaviours. A particular absence in the literature is any attempt to understand the nature of photographs of children, or their significance for the user."

This observation is confirmed by the results of the questionnaire sent to the member states of the Council of Europe. Most of the persons contacted replied that, so far, no studies/research had been undertaken in their respective countries on persons using NCITs with a pornographic/sex-related motivation, with the exception of a German study carried out in 1997 on child pornography by the Federal Office of Criminal Police in Wiesbaden, and the data from the European Centre for missing children "Child Focus".[3] *It would then be very important to have research developed on the item of consumers.*

As regards *offenders*, Ms Hughes described the different types of offenders in her study. One important issue is that most start out accessing adult pornography, then move on to child pornography. They continually move up to more sophisticated technologies and more sexual exploitation of children, either in seeking more harmful, extreme images, or the physical sexual abuse of children.

The offenders deny the harm they are doing to children and women. In this case, as Ms Gerstendörfer noted it, the use of language can also be very important. "Language reflects and creates reality" (cf. Wittgenstein). Pedocriminals are calling themselves "paedophiles" ("paedo", Gr. child, boy; "phil", Gr. beloved, esteemed, cherished). This is dismissing as trifling, it also tries to "re-define" values of our societies: many pedocriminals compare their so-called "sexual orientation" to homosexuality, which in fact was defined as "sexual deviation" in former times. At the same time, pedocriminal organisations try to get an official non-profit status for their "self-help" groups.

The group of experts stressed the importance of using language that showed that the actions concerned were criminal, for instance, "pedocriminal" instead of "paedophile".

Mixing up the categories "sexuality" and "violence" does, however, support perpetrators and their excuses ("instinct", "desire", "helplessness", etc.). Perpetrators are abusing this symptom

3. See document EG-S-NT (2001) 7.

as an excuse for their criminal act, stating that they have been seduced by the victim. This analysis is shared by Ms Hughes who says that the biggest problem in combating trafficking for the purpose of sexual exploitation is the denial of the harm to women and children:

> "The users who sexually exploit women and children defend their rights and actions. They frequently portray themselves, even child sex abusers, as victims of oppression and intolerance. In the users' view, groups opposing sexual exploitation and even child pornography are attempting to oppress the users' right to pursue their pleasure and express their 'love' for children."

Ms Hughes also said that society has become accepting of these images of sexual exploitation, and no longer questions them. Even law enforcement officials dedicated to fighting trafficking for the purpose of sexual exploitation often use pornographic language and terms to describe what is done to the women and children. In doing so they become complicit with the traffickers and users in the denial of the harm by minimising or eroticising the actions of the perpetrators.

The denial of the harm in attitude, policy and practice has resulted in there being no points of reference or standards to evaluate the images or understand the coercion going on behind the smiling faces of the women and children.

4. Protection of the victims

Concerning the protection of the victims, the group recalled Recommendation No. R (2000) 11 of the Committee of Ministers on action against trafficking in human beings for the purpose of sexual exploitation[1] and Recommendation Rec (2001) 16 on the protection of children against sexual exploitation condemn trafficking in human beings for the purpose of sexual exploitation as a flagrant violation of human rights and an offence to the dignity and integrity of the human beings. They state as an essential goal the adoption of legislative measures and actions to "the protection of the rights and interests of the victims of trafficking for the purpose of sexual exploitation, in particular the most vulnerable and most affected groups: women, adolescents, and children". They give absolute priority to assisting victims of trafficking for the purpose of sexual exploitation through rehabilitation programmes, and to protecting them from traffickers.

1. See Appendix 8, p. 83.

C. Prevention

Concerning the prevention, the actual history of new information technologies and human rights violations must be taken into account. But, according to Ms Hughes, most of experts only have partial information. The only people who have knowledge of both computer technologies and sexual exploitation are those investigating child pornography or child stalking, but they know little about trafficking for sexual exploitation of prostitution or adult sexual exploitation. A fundamental knowledge of the development of this problem and its pro-active factors over the last decade could help to raise awareness (mistakes committed for empowering criminals, non-reactions, good practices of NGOs) and understand the whole complexity of the problem as well as the measures which should be taken.

Nevertheless, according to Ms Gerstendörfer, most concepts of "prevention" are not real prevention, but "security belts" after violence has happened.[2] Understanding demands to see all the different perspectives. The group of experts proposed thus that preventive measures should first aim at effectively controlling the Internet, with codes of good practice, filtering systems, etc.

But for some researchers, proposals for a European network of hotlines, filtering and rating systems, self-regulation, codes of conduct, encouraging awareness actions and assessing legal implications will allow people to stop seeing the abuse of women, *but it will in no way eliminate the abuse*. Such a policy is inadequate to stop the pimps and predators on the Internet. Prevention also means to implement *short-term and long-term measures* at the same time. *Short-term measures* are passive prevention, *long-term measures* are active prevention. There must be a co-ordination between both, for example via priority lists – and their continuous evaluation – of what has to be done, when and by whom.

Short-term measures against perpetrators should be taken, because they have full responsibility for all the economical, psychological and other "costs" for individual victims and the whole society and for compensating the harm made to the victims. One possibility is to seize and confiscate the benefits from trafficking for the purpose of sexual exploitation, as provided in paragraph 44 of Recommendation No. R (2000) 11 of the Committee of Ministers to the member States of the Council of Europe:

> "Take such steps as are necessary to order, without prejudice to the rights of third parties in good faith, the seizure and confiscation of the instruments of, and proceeds from, trafficking for the purpose of sexual exploitation."

The explanatory memorandum develops this idea:

> "In addition to financial assistance to cover the cost of the return journey and a sum of money to aid reintegration, victims could be provided with the means of settling their debts, in the form of a compensation scheme or any other suitable system for settling debts (possibly based on confiscation of the proceeds from trafficking for the purpose of sexual exploitation, as provided for in paragraph 44)."

Prevention should focus on two aspects:

- Prevention *against victimisation* of women and/or children; and
- Prevention *against violent behaviour* of men and/or members of criminal organisations.

This second type of prevention focuses on education within families, schools, universities, media, etc. It is linked to the social climate and its impact on individuals and groups within our societies. Such distinctions are important to develop and implement more effective strategies.

2. See Hageman-White 1992.

Who can and must prevent?

The question "who can and must prevent?" is an important one, and also needs an explicit analysis. The cost paid by the victims is very high and has economical, psychological and social consequences. Therefore, this problem, which is first of all a human rights violation, should be considered as a high priority for the society and for the governments. To this end, public authorities should give priority to cases involving trafficking for the purpose of sexual exploitation. They must be dealt with as quickly as possible in a way which is compatible with the rights of all the parties. Offences relating to trafficking for the purpose of sexual exploitation do not always receive from the public authorities the priority that the gravity of these crimes requires. In many countries, as Mr Walraet underlined it in his study on law enforcement and cases, legislators and decision-makers are often oblivious to what really is happening on Internet and must be made aware of the issues involved.

Professionals, public authorities, organisations and civil society must be involved at their respective levels and work in co-operation in order to combat and prevent this phenomenon. Ad hoc measures should also be taken in order to give all the partners the means to better understand the problem:

- Set up assistance programmes for the victims including therapies, employment opportunities, etc.; support research in the field of prevention of trafficking for the purpose of sexual exploitation via the new information technologies and in the field of the prevention of violence.
- Law enforcement and judiciary should be trained on trafficking for the purpose of sexual exploitation via the new information technologies, in particular judges should be trained to understand the psychology of the victims and work in co-operation with NGOs and law enforcement; journalists should be trained in order to inform the public on trafficking for the purpose of sexual exploitation without sensationalism and to avoid stereotypes.
- NGOs should develop and implement assistance programmes for the victims, launch awareness campaigns against trafficking for the purpose of sexual exploitation and campaigns against stereotypes; the media and public authorities could help them to find "sponsors" to support them.

Combating illegal and harmful actions through new technologies

As far as the prevention of misuse of NCITs is concerned, in some countries, which replied to the questionnaire, measures have been taken, such as hotlines, but it appears that information and awareness-raising campaigns have been the most efficient.[1]

Examples of good practices were also mentioned. In Denmark, the association PORCH was founded by parents in order to try to identify and arrest pedocriminals who contacted children through the Chat rooms. In Belgium, the MAPI project was set up by researchers and academicians of the Namur Institute for Computer sciences of the University. MAPI, (*Mouvement Anti-Pédophilie sur Internet*/Anti-pedophile movement on the Internet) is a research group which studies the questions related to the availability on Internet of information encouraging sexual exploitation of children; the group conducts research, awareness-raising actions targeting the users and suggests recommendations. In May 2002 the BBC launched a new type of Internet search engine which uses a software to remove pornographic material from the search database.

Also the questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services distributed in preparation for the forum held on 28 November 2001,[2] updated in April 2002, mentioned the existence of codes of conduct in ten member states of the Council of Europe.[3] Others have common rules, observed by industry members, having no legislative or regulatory basis but complying with the international law in force. On the whole, the codes are binding on members of the organisations concerned, subject to penalties

The replies to the questionnaire on self-regulation and user protection against illegal or harmful content on the new communications and information services also described other control measures in respect of providers and content such as:

- organisations representative of Internet industry players: they ensure that Internet stakeholders' efforts are better channelled;
- regulatory bodies: they have a supervisory role with a view to preventing and/or punishing abuse by service of content providers.

Filtering systems were also mentioned. The existing systems are:

- **blacklisting** (software that blocks access to certain sites)
- **whitelisting** (definition of sites to which access iss allowed)
- **rating of sites** by category.

With regard to the filtering systems currently in existence, the group found that it would be interesting to study the use made of them, as well as alternatives. Some replies were found in the 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: rating of content is less widespread, but an international initiative exists in this sphere: ICRA (The Internet Content Rating Association). Various measures are implemented by the countries: voluntary use of labelling and filtering of content; access providers have to inform their subscribers of the means of filtering that exist and to offer them at least one such means; information sites about the means to protect children; empower users to download a content.

As regards the content labelling issue, a rational approach must be adopted, taking into account the requirements of the European Convention on Human Rights, in particular Article 10 on freedom of expression and information. This is stated expressly in paragraph 6 of the Appendix to Recommendation Rec (2001) 8.[4]

1. See document EGS-NT (2000) 10: Denmark, Russia, Finland, Croatia, Hungary, Latvia, Slovenia, Czech Republic, Romania and the United Kingdom describe their national experiences.

2. Summary and analysis, last update: 24 April 2002, Group of Specialists on on-line services and democracy (MM-S-OD). 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.

3. Austria, Belgium, Bulgaria, Canada, Italy, Spain, United Kingdom and Hungary in connection with a representative organisation; Spain again, Norway and Germany in connection with a regulatory body.

The group noted that much information was available on the "abuse" of the Internet, but people did not know how to react or whom to contact. Users must be aware of complaints systems' existence and know how to use them. A number of official points of contact did exist and could serve as "clearing houses", but awareness-raising measures were needed to inform people about the possibilities at their disposal. For instance:

- a directory of useful sources at European level should be published;
- an Internet user guide for parents and children should be produced;
- a Web site with useful links should be created;
- the activities of NGOs involved in work of this kind should be supported;
- the Belgian example of the European centre for missing children should be followed elsewhere;
- user-friendly telephone help lines ("freephone numbers") should be made available.

Finally, given the ease of the methods of payment on the Internet, the group wondered whether there were ways of "countering" firms which collaborated with sites that sexually exploited women and children. Until there had been a court ruling, it seemed that it would even be illegal in certain cases for such firms to refuse to provide services.

4. Recommendation Rec (2001) 8 of the Committee of Ministers to member states on self-regulation concerning cybercontent (self-regulation and user protection against illegal or harmful content on new communications and information services) – Chapter 2 – Article 6: Member states should encourage the definition of a set of content descriptors, on the widest possible geographical scale and in co-operation with the organisations referred to in Chapter I, which should provide for neutral labelling of content, thus enabling users to make their own judgment concerning such content.

D. The role of the mass media

The group decided to look at how the media could play a key role in raising public awareness of the issue of trafficking in human beings for the purpose of sexual exploitation and new technologies and contribute to prevention. It agreed that the matter needed to be considered in detail, as self-regulation of the media was a sensitive issue.

Ms Sigrun Stefansdóttir,[1] journalist and member of the group, was asked to examine the question on the role of the mass media. It is completed by the information gleaned from the questionnaire replies and some conclusions from the Workshop on "good" and "bad" practices regarding the image of women in the media – the case of trafficking in human beings for the purpose of sexual exploitation.[2]

In most replies to the questionnaire, the role of the media is quoted as being very important.[3] The mass media do not only have an awareness-raising role to play towards the public, but they can also stimulate public debate and provide an incentive to the adoption of political measures to combat this new form of crime.

The role of the mass media, with regard to its influence on public ethics and dogmata, is pivotal in modern democracies. The press has the task of not simply informing and entertaining, but also of educating. Therefore, the public press has authority and responsibilities that extend beyond petty self-interest and which should preclude the pandering to crass commercial or political interests, which we see too often in both state-operated and private media. This applies especially to public service broadcasters and other civically oriented media, who have a responsibility to not merely avoid but also prevent the propagation of illegal and/or harmful material, such as material promoting sex trade of any type.

The media obviously has an enormous capacity to shape public thinking. But how is the press using this potential within the sphere of cyber-crimes involving trafficking in human beings for the purpose of sexual exploitation? How do the classified sections of newspapers filled with sex advertisements affect the investigative journalism – or the lack thereof – focusing on the rapidly growing international problem of trafficking in human beings for the purpose of sexual exploitation? How does the press reach a balance between freedom of expression and a code of ethics on the one hand and between morals and profits on the other? How does the definition of what is news apply to cybercrimes and vice versa?

Those questions are among a number of matters that needs to be addressed when defining the role and responsibly of the mass media in the fight against the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation.

1. Dr Sigrun Stefansdóttir, Informationschef, NMR/NR.
2. Held in Strasbourg, 28-29 September 1998. See document CDEG/CDMM (98) 10.
3. See document EG-S-NT (2001) 9.

Where are the blockages?

The money matters

Money matters. A big part of the revenues of newspapers come from the sale of advertisement space. Indeed, revenues from commercial sex advertising represent a significant income for certain papers.

A study carried out in Finland in 1999 by Ms Mari-Elina Laukkanen showed that out of 35 newspapers examined, 24 published commercial sex advertisements. The biggest selling daily newspaper, *Helsingin Sanomat*, which is a highly regarded paper, seemed to lead the field in terms of the volume of published sex ads. During the week of examination the paper published some 900 advertisements promoting sex services. This study was conducted as a part of the national "Programme for the Prevention of Prostitution and Violence against Women" and the primary objective of the study was to highlight the money flow related to commercial sex advertising and its significance for the economy of the Finnish daily press.

The Finnish press is, however, no worse or no better than the press in other countries. Indeed, *Ekstra Bladet* in Denmark profited from selling a total number of 425 advertisements promoting sex trade in a single day in May 2002, covering over three pages. That same day, *Dagbladet* in Norway, which claims to be

a serious, critical newspaper, sold space for sex ads covering a whole page and, similarly, *DV* in Iceland sold one-and-a-half pages.

Ms Laukkanen concluded the following in her paper entitled "Ladies for sale: the Finnish press as a profiteer":

> "The sex trade uses marketing effectively in order to normalise the consumption of the products and service it offers as an unquestioned part of ordinary life and the public sphere. With its prevailing policy regarding sex advertising, the daily press contributes to this process of neutralisation of the sex trade, where mostly women have become sexually stimulating products to be sold, bought and consumed. The press can be demonstrated to be an institution that perpetuates the sex industry by offering a forum for sex advertising."

Ms Laukkanen sees the press as a reinforcer of prevailing cultural values and as a constructor of social reality, rather than as a neutral mediator of new information. In her study, she also claims there is a tendency for the language in sex advertising to become increasingly graphic. Marketing lines that suggest that sexual harassment or abuse is taking place in professionally confidential relations has also been established as a part of commonly used marketing themes of the sex trade. In the advertising of sex service providers, women are identified as objects at many levels: a product of the sex trader, as an object for the spectator of the ad, and as a tangible object for the purchaser.

This problem of classified advertisement was also examined during the workshop on the image of women in the media.[1]

> "While those sexually exploiting women can use the Internet as a means of exchanging information, it is through classified advertisements in the printed press that most women start their harrowing journey into exploitation and forced prostitution."

During this workshop it was reported that media owners and managers of their advertising departments argue that it would be impossible to check every classified advertisement that is posted in the newspaper. They need to be alerted by local police investigating traffickers. But police are often complacent about the issue or not sufficiently equipped to deal with the problem.

It was then proposed that while media cannot be made liable for the contents of classified advertisements. They could adopt a code of practice that requires them to reject those advertisements that are easily identified as aimed at luring women into prostitution. A more vigilant advertising policy should be adopted. For example, the International Federation of Journalists (IFJ) at a world conference on Media and the Rights of Children which took place in Brazil in May 2000, endorsed the following statement:

> "The IFJ is deeply concerned at the creation of paedophile Internet sites and the fact that certain media publish or broadcast classified advertisements promoting child prostitution.
>
> The IFJ calls on its member unions to: intervene with media owners over the publication or broadcasting of these advertisements; campaign with public authorities for the elimination of these sites and advertisements."[2]

Ms Sigrunsdóttir also raised the following question: How can the mass media critically fulfil its role in the raising of awareness about the growing impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation when, at the same time, the media contributes to this process by offering a forum for sex advertising and thereby actively contributing to the neutralisation process of the sex trade?

This conundrum manifests that self-regulation performed by most newspapers is not adequate. Therefore, restriction measures must be given serious consideration. Indeed, there is a need to strike a balance between freedom of expression and a code of ethics, and between morals and money.

As regards codes of ethics, it was underlined during the workshop that sometimes genuine conflicts arise between values, and confidence of ethical decision-making is required. In her review of 28 codes of ethics in 26 European countries, Tiina Laitila found that 86% made reference to the use of fair means in information collection.[3] However, the definition of "fair" is open to debate. Deciding when the public interest becomes "overriding", and what "other means" are permissible, is left up to the conscience of the journalist, or often to the employer. This clause affirms that journalists are *entitled to exercise a personal conscientious objection to the use of such means.*

While codes of conduct and guidelines appear not to be effective, they can be useful in demonstrating that something needs to be done. Such codes are weapons in the hands of journalists and campaigners who can use them to take up issues with editors, publishers and broadcasters. Also codes of ethics can be useful in order to avoid disagreeable situations when dealing with cases of trafficking in human beings for the purpose of sexual exploitation.

Within media, standards of professionalism should be promoted that will assist journalists in addressing the ethical dilemmas they confront when reporting on sexual exploitation of adults and children.

The news values

For generations journalists have used similar criteria in deciding the news value of each day's tidings. That is, to decide which among the seemingly infinite numbers of events, ideas, and continuing controversies should be reported in the media on any given day. Various editors, teachers and textbooks use varying protocol for those decisions, but almost every journalist's list is similar to this one:

- **Impact** - how many people an event or idea affects and how seriously it affects them determines its importance as news.
- **Proximity** – the closer that an issue or an event is to your audience, the greater the impact and news value it will have.
- **Timeliness** – today's news is stale tomorrow.
- **Prominence** – names make news; the bigger the name, the bigger the news.
- **Novelty** – the unusual, the bizarre, the first or last or once-in-a-lifetime event is news.
- **Conflict** – war, politics, and crime are the most common news of all.

Those six elements work both for and against the subject of trafficking in human beings for the purpose of sexual exploitation. Mr Roland Walraet from the Federal Computer Crime Unit

1. See doc. CDEG/CDMM (1998) 10.
2. See doc. CDEG/CDMM (1998) 10.
3. Tiina Laitila, *The journalistic codes of ethics in Europe*, Dept of Journalism and Mass Communication, University of Tampere, 1995.

(Belgium) illustrates the difficulties encountered by investigators in pursuing criminals on the Internet, due to the lack of sufficient mechanisms for co-operation between European police forces. This is largely due to a lack of possible actions that can reasonably be taken by the cyberpolice officers, due to the differences in legislations and the fact that they have not extraterritorial authority to investigate. These aforementioned elements make the investigations often time-consuming and frustrating for the cyberpolice:

- When did the cybercrime actually take place?
- Who are the criminals?
- Where are they?

These questions are not always easy to answer. Those very same elements often make it difficult for the media to cover the story. The journalist needs an actor, a name and a face, here and now. The news story has a narrow framework, governed by time on the air or the space on a page. The elements in the cybercrime story are often too numerous to be incorporated into the typical news-frame. They fit badly into the black and white framework of the news writing.

The modern trend in the journalism of today is the personalised style whereby the journalist seeks a story with a clear focus on a person – a hero, a victim, or a criminal.

Coverage of trafficking in human beings for the purpose of sexual exploitation often focuses too much on the individual whose case provides the news angle. Media need to broaden the scope of reportage. The story of sexual exploitation in general and its commercial aspects in particular is not being told in full. To examine how this can change requires a look at the professional freedoms which journalists require to work effectively, a summary of the principles or guidelines journalists and programme-makers should follow, and the pressures – legal, financial, or cultural – which are standing in the way.

This idea was also developed during the workshop by Ms Peters, in her statement on "Raising awareness or sensationalising: a two-edged media knife":

> "Many western European public service channels have broadcast documentaries on the issue and one can find reports on trafficking for the purpose of sexual exploitation and forced prostitution in most newspapers across Europe."

The important role these reports can play in raising public awareness of trafficking for the purpose of sexual exploitation in women is well understood. But the issue is not as clear-cut as many would like; while media coverage can shine the spotlight on those directly responsible, the victims are all too often also caught in the glare of publicity.

Some of the findings of the report of the Council of Europe's Committee on Crime Problems,[1] which dealt with sexual exploitation and trafficking in children and young adults for the purpose of sexual exploitation, also apply to reports on trafficking in women for the purpose of sexual exploitation. They warned:

> "Often the mass media function as a two-edged knife in this area of concern. The unravelling of sensational sex and crime cases involving children and young adults tends to overemphasise the issue and to blur the picture. Sometimes, though, it is the media which help to uncover cases of sexual exploitation and to raise awareness of the problem.
>
> But it is also the media that generally infiltrate the public with liberal and tolerant attitudes towards child pornography and prostitution or provide the ways and means (for example advertisements) by which this sex gratification may be achieved. Therefore, their co-operation and their orientation towards safeguarding the rights and the dignity of children and young adults is extremely important."

Media researcher Nancy Signorielli sees two sides to sensationalism:

> "Although human rights advocates may argue that sensational coverage distorts and exploits a serious problem – perhaps doing more harm than good – sensationalism solves several editorial problems; that is, it can be the response of reporters and editors trying to fulfil the responsibility to cover serious social issues, while continuing to turn a profit. Sensationalism permits an important but unpleasant topic to be covered in such a way that it still captures the readers' attention - and sells magazines."[2]

In spite of the criminality of trafficking in human beings for the purpose of sexual exploitation, the aforementioned aspects of the news criteria hinder the mass media in being an effective tool in the fight against cybercrime, as well as playing a role in increasing the general awareness of the problem.

1. Council of Europe, Select Committee of Experts on sexual exploitation, pornography and prostitution of, and trafficking for the purpose of sexual exploitation in, children and young adults.
2. Nancy Signorielli, "Magazine Coverage", in Gerbner et al., *Abuse, an Agenda for Action*.

New approaches

Ms Sigrunsdóttir proposes new approaches to the question, which are democratic control of the media, social responsibility of the media. The workshop also proposed some ideas concerning the training of journalists which are also presented here.

Democratic control of the media

In the final report of activities of the Group of Specialists on Future Priorities, Strategies, and Working Methods in the Field of Equality between Women and Men (October 1999), freedom of expression is referred to in the following way:

> "Freedom of expression is not a privilege of the press, but a fundamental right of all citizens; the press in all its forms is an important indicator of citizens' freedom of speech and thought, and itself a vehicle for its growth and full use. At the same time, the press has also become profoundly intertwined with advertising, which, in itself, is essentially an economic activity in the market economy, quite different from the expression of opinions or the public debate of issues. The need to regulate advertising has been long recognised in democracies. [...] Regulating advertising may indeed protect the freedom of the press."

Thus there is no sense in confusing freedom of the press with "auto regulation" (or "internal jurisdiction") advocated by some within the advertising industry. Three sources of norms are conceivable for this branch of activity, namely:

- external norms and/or incentives by public authorities
- internal ethical committees for auto regulation
- customer mobilisation setting limits to advertising that offends significant numbers of people, as has been employed with respect to sexist presentations.

This applies directly to the realm of the media's role in trafficking for the purpose of sexual exploitation in human beings for the purpose of sexual exploitation. Indeed, combinations of the above norms (depending to some extent not only on local traditions and sensitivities, but also on pragmatic considerations) need to be further brought into play with the ultimate goal of setting limits to the reinforcement of advertisements promoting sex services, which leads to a double standard of the press.

The social responsibility of the media

Faced with an increasingly complex reality and an almost inescapable apprehension of a world that is perpetually made more complicated by advancing technical processes, the media finds itself assigned a role of considerable gravity. In that role, public service broadcasters, not being subject to the same strains of commercial logic as their private counterparts, can provide models for other media and should continue to be a fertile source of original ideas. In fact, a leading role in educating the public about the various issues and aspects of the new forms of communication and information services, present and future, is required from the media. With the responsibility of the role as educator, however, arise the obvious needs for increased emphasis on the training and guidance of members of both the new and traditional media, as well as the increased availability of reliable and approachable academic research results. These aspects obviously need to be configured to operate concurrently and in tandem with changing technological trends to avert utilitarian stagnation and unawareness of the issues at hand. That is, these aspects need to be as continuous and reactive as feasible.

Modern schools of journalism are not the isolated cells they once arguably were. Today they also offer knowledge, training, service and research results to society as whole, including the media, general public and government. The critical education that these schools of journalism offer makes new journalists attentive and well-prepared professionals, ready and equipped to use their technical knowledge to promote journalistic information as an instrument of learning and thus of democracy. But it must be stressed that gender awareness cannot be too highly emphasised in these media and occupational training courses must therefore absolutely not be neglected. Indeed, this issue should not merely be treated as a special topic, but infused into all aspects of journalist and media training. Furthermore, professional organisations and networks need to assess their roles in education, advice, and raising awareness.

The conclusion is that the following four sources are conceivable for making the press play a more active and responsible role in the fight against cybercrime and creating more public awareness:

- Increased emphasis on the leading role of the modern schools of journalism in raising gender awareness in the broad meaning of the word.
- Increased emphasis on teaching new journalists about the structure of international organised crime and the fight against it, through international organisations.
- Increased emphasis on the leading role of the media itself as the fourth estate in modern society.
- Increased availability of reliable and approachable academic research results on the issue of trafficking for the purpose of sexual exploitation

Training for journalists

During the workshop on good and bad practices regarding images of women in the media, participants underlined that *ethical questions should have a higher profile in journalists' training*, particularly with regard to standards of conduct in reporting issues like adults and children's sexual exploitation.

The participants in the workshop also underlined *the need for better co-operation between media, police and NGOs involved in the fight against trafficking in human beings for the purpose of sexual exploitation.* Both national and European authorities have vouched to educate young women about the dangers of working abroad. Media in the countries of origin of the exploited women could work with police and organisations in civil society in providing women with information about the risks involved. Media have a role to play in making the general public and often the police understand that these women are not criminals but victims of exploitation.

The Council of Europe could support initiatives that bring together media professionals, police and civil rights organisations to create better co-operation in the fight against trafficking for the purpose of sexual exploitation and sexual exploitation of women.

The mass media do not only have an awareness-raising role to play towards the public, but they can also stimulate public debate and provide an incentive to the adoption of political measures to combat this new form of crime.

Having taken into account the information put at its disposal on the role of the media, the group also made some proposals concerning this role:

- Civic duty is also a mean for fighting for journalists and NGOs, but they must very cautious not to destroy the work undertaken by the police to find the evidence.
- As regards publicity: the research demonstrates that more the programmes have sexual and violent contents, the less the publicity stays in memory. The idea that sexual and violent programmes help to sell is wrong and should be promoted among the media.
- The way media report on campaigns against trafficking for the purpose of sexual exploitation should be evaluated. For example how the local media followed the campaign "Sold like a doll" in the Baltic countries should be used as a case study in the training of journalists.
- To avoid stereotypes with regards to women and avoid sensationalism when reporting on trafficking in human beings for the purpose of sexual exploitation.

E. Freedom of expression and the Internet

The growth in crime and unlawful practices connected with Internet use is proof that public authorities cannot eschew all regulation in this area, in the name of freedom of expression, in particular when Internet is used for what is considered as a gross violation of human rights, trafficking in human beings for the purpose of sexual exploitation. The question is, what kind of legislation is needed to regulate the Internet, and what other forms of control are there, apart from laws and regulations?

In a report on regulating the Internet and violence against women, Ms Loni Bramson[1] said that the excuse given for allowing violence against women on the Internet is *freedom of expression*. There is clearly a clash of standards between the freedom of expression, enshrined in Article 10 of the European Convention on Human Rights (ECHR) and other rights threatened by violence or trafficking for the purpose of sexual exploitation used to produce images broadcasted on Internet: the right to life in Article 2 of the ECHR, the right not to be subjected to torture or to inhuman or degrading treatment in Article 3 of the ECHR, and the rights of private life, free speech, human dignity, freedom from violence, etc. Should service providers, site managers, those setting up illegal pages or any other user be punished, even if they are not responsible for the content of the sites under their control? Should users be put on file, notwithstanding the concerns this would raise in respect of computer laws and freedoms?

For Ms Bramson, engaging in a discourse to protect women from becoming part of harmful or illegal content or from being victimised on the Internet is almost impossible. The discussion regarding regulating the Internet should be seen for what it really is, one of values. Who has a priority in rights? Is it the predators who claim freedom of expression to hurt and exploit women and place the results on the Internet, or is it women who have the higher right to not be harmed, violated and exploited?

Ms Bramson says that the European Union proposal for a European network of hotlines, filtering and rating systems, self-regulation, codes of conduct, encouraging awareness actions and assessing legal implications will allow people to stop seeing the abuse of women, *but it will in no way eliminate the abuse*. Such a policy is inadequate to stop the perpetrators on the Internet.

Ms Hughes also said that in connection to the use of new technologies, there is fatalistic assumption that nothing can be done when it involves the Internet. Because of the libertarian culture on the Internet and the lack of intervention in the past, people have developed the attitude that it is not possible to stop anything. People often believe that the Internet cannot be "censored", that it is impossible to intervene in any way.

As regards the freedom of expression, Judge Gomez, who has been responsible for the Yahoo! case, considered that the criminal and illegal activities that are growing more widespread on the Internet proved that it is impossible to avoid introducing some form of legal control over this new medium in the name of freedom of expression. But the group considered that judges could not be expected to control the Internet in particular, and the new information technologies in general, on their own. It proposed that preventive measures should first aim at effectively controlling the Internet.

The conclusions of the Forum on harmful and illegal cybercontent organised on 28 November 2001 by the Council of Europe in Strasbourg also focused on education, self-regulation and the need of co-operation. It brought together renowned experts in the field of Internet regulation and the fight against illegal content on the World Wide Web. Through the organisation of the Forum, the Council of Europe aimed to provide an operational follow-up to its Recommendation (2001) 8 on self-regulation concerning cyber contents.

This Forum analysed different ways of regulating the Internet, in particular self-regulation by the industry and co-regulation, whereby public authorities and the private sector co-operate. The Forum also looked at how users of the Internet can be empowered to protect themselves and their children against harmful and illegal content.

If the participants reached a consensus on some issues, such as the necessity to preserve freedom of expression, the emphasis on education and the need of co-operation and a cross-media and cross-platform approach adapted to different types of media, the debate on questions such as illegal and harmful content and how and who should regulate these contents, had been a lively debate on two differing approaches: freedom of expression and regulation.

The conclusions of this forum showed that there is a broad consensus on some themes such as the protection of children in all cases, both as users and as victims, *but the question of the women victims of trafficking in human beings for the purpose of sexual exploitation for the purpose of sexual exploitation on Internet does not seem to be a priority.* Questions of what should be illegal content and what content, though legal, should be regulated because of its harmful nature to children were considered as public questions. They must be openly debated and not merely delegated to private and privatising technologies that are neither transparent nor accountable.

The Internet, like television before it, is a public medium with far-reaching social implications. Content issues should be treated as matters of public concern.

Education was also considered as a key element in recognising dangerous content. Reference had also been made to filters used for monitoring purposes and those which could be installed by users.

Certain matters undeniably needed to be regulated, however, it is difficult in a global network to take account of local values and to draw the line between what is lawful and what is unlawful, which is why it is necessary to co-operate in this field.

1. Loni Bramson, PhD, MAPP, February 2001, "Regulating the Internet and violence against women".

Conclusions and recommendations

A. Conclusions

In accordance with its terms of reference, the experts have studied the impact of new information technologies on equality between women and men and in particular on trafficking in human beings for the purpose of sexual exploitation. They developed a global approach and studied the different kind of new technologies, how they are used, who are the users and the victims. They studied how the question of Internet linked to trafficking for the purpose of sexual exploitation was considered through national laws and international treaties and how to fight against the illegal and harmful content of Internet. They also examined the question of the violation of human rights and the consequences for the victims in relation with the question of freedom of expression.

On the basis of the results obtained, the group of experts underlined the *usefulness* of Internet and of the new information technologies in general. The fact that Internet is a global network presents various advantages, including also the possible use of the technology to better fight organised crime or to help the victims. However, it appears that the new technologies are largely *misused*. None of these new technologies are in and of themselves harmful, but they provide those who wish to harm or exploit women and children with new, efficient and, *often anonymous*, ways of doing that.

The Internet industry and the sex industry are closely interlinked and the scope, volume and content of the material on the Internet promoting or enacting trafficking in human beings for the purpose of sexual exploitation in human beings for the purpose of sexual exploitation are unprecedented. The growth of shadow economies and transnational criminal networks are negative manifestations of globalisation arising from expanding economic, political and social transnational linkage which are increasingly beyond local and state control. *It can be said that if the use of new technologies may not have increased the trafficking for the purpose of sexual exploitation of people, it has made the activities easier and introduced new ways of trafficking in human beings for the purpose of sexual exploitation.* As more cases of trafficking for the purpose of sexual exploitation are uncovered, the details of their operations will mostly like reveal an increased use of electronic communications.

Privatisation creates wider and more open marketplaces throughout the world, and the phenomenon is certainly boosted by a strong *demand* factor. Another important component of globalisation, computer communications technologies enable the increased volume and complexity of international financial transactions, which increase opportunities for transactional crime and decreased the probability of detention and apprehension. This technological aspect of globalisation enable the money gained through illegal activities to be transferred and laundered in any country.

The growth of these phenomena is also due to the *inexpensive* and *accessible* nature of new technologies. Various kinds of technologies can be used for the purpose of sexual exploitation – either by individuals for their own private use or by persons or groups using the Internet as a commercial tool, to promote and sell images or services.

Technology is providing new ways to traffic women for the purpose of sexual exploitation and new ways to transmit the images of sexual exploitation. Often, the geographical location of the server (which can be situated in countries where the legislation in the field is weak or absent) *neutralises the law.*

Legislation on the Internet is still very much in its infancy, and the difficulty of legislating in this area is compounded by the fact that the Web transcends national borders.

At international level there is no effective internationally approved instrument on the content circulating on the Internet linked to trafficking in human beings for the purpose of sexual exploitation. *There is clearly a need for a minimum of common and effective international standards for collecting evidence and prosecuting cases and for co-operation between countries at legal, technical and judicial levels.*

The experts noted that there is a growing disparity between the attitude of the law towards child pornography, which is categorically banned in most European countries, with access providers being forced to shut down certain websites, and its attitude towards trafficking in adults for the purpose of sexual exploitation, such as the production of adult pornography and mail bride orders.

In the case of trafficking in adults for the purpose of sexual exploitation, the law is much less clear and legal action less effective. NGOs state that women who find partners through marriage agencies are at higher risk of becoming victims of violence and exploitation, *but more research in this field is needed.* It is

important to be able to document, through a few cases of trafficking for the purpose of sexual exploitation, that harm to women goes beyond domestic violence to trafficking for the purpose of sexual exploitation of adults, such as the production of adult pornography and mail bride orders. Research should be developed on this issue and marriage agencies should be included in prevention and awareness programs against trafficking in human beings for the purpose of sexual exploitation.

It should be noted, as regards actions and cases, that examples of action against trafficking in human beings for the purpose of sexual exploitation via new information technologies appear to be more common in the field of child pornography than in cases involving the exploitation of adult pornography or the exploitation of prostitution.

Through the use of new technologies, new sex-related businesses are opening up and facilitate the trafficking in images of women and children for the purpose of sexual exploitation.

The use of new information technologies for trafficking in human beings for the purpose of sexual exploitation *creates different kinds of victims,* such as victims of domestic violence, whose images are circulating on Internet, and victims of different kind of offenders, such as involuntary users, often minors, in some cases lured into the business through harmful use of technologies by traffickers. Prevention, protection and rehabilitation of the victims should be considered as *a high priority* for the society, policy and decision-makers.

Questions of what should be illegal content and what content, though legal, should be regulated because of its harmful nature are public questions. The Internet, like television before it, is a public medium with far-reaching social implications. Content issues should be treated as matters of public concern. The role of the media to raise public awareness in order to prevent and combat the phenomenon of trafficking for the purpose of sexual exploitation through the use of new technologies should be essential. The experts stressed the necessity for the professional organisations and networks to assess their roles in education, advice and raising awareness.

The growth in crime and unlawful practices connected with Internet use is proof that public authorities cannot eschew all regulation in this area, in the name of freedom of expression, in particular when Internet is used for a gross violation of human rights, which is trafficking in human beings for the purpose of sexual exploitation.

The use of new technologies for the purpose of sexual exploitation of human beings presents new challenges to lawmakers, law enforcement, and international cooperation. The question is, what kind of legislation is needed to regulate the Internet, and what other forms of control are there, apart from laws and regulations?

The challenge is to change attitudes, policies and laws that connect the acts and images in ways that preserve rights of freedom of expression, but protect the rights of women and children to be free of criminal acts of trafficking in human beings for the purpose of sexual exploitation.

There is certainly a need to strengthen the measures and legislation at national and international level, priority being given to the prevention and protection of the victims, the promotion of equality between women and men, develop education and training in order to give to the actors in any field concerned by the problem the tools to prevent and combat effectively and efficiently the trafficking in human beings for the purpose of sexual exploitation and set up close co-operation at national and international levels between the bodies working in the same field.

In order to better fight effectively the impact of the use of new technologies on trafficking in human beings for the purpose of sexual exploitation, the experts made the following proposals on these different issues.

1. The need to strengthen measures, legislation and implementation at national and international levels

There is not always a specific provision in the national criminal legislation prohibiting trafficking in human beings for the purpose of sexual exploitation, however, it is sometimes deemed to fall within the definition of other more general crimes. The current trend is to introduce a specific norm which defines trafficking in human beings as a criminal offence in and of itself because existing norms are not sufficient. Where there is such a specific provision, there is a clear intention to punish trafficking in human beings for the purpose of sexual exploitation, but the exploitation for other purposes is not regularly included in the prohibitions, *the member states should review their legislation in order to prohibit and penalise trafficking for the purpose of sexual exploitation in persons.*

There is no need to adopt new legislation specific to the use of new information technologies for the purpose of sexual exploitation in countries where new provisions were included in existing national legislation considering the use of new information technologies for the purpose of sexual exploitation *as an aggravating circumstance which increases the applicable penalties.*

In all the relevant countries sexual activities concerning in particular the prostitution of minors and children are punished more severely. Traditionally, that which was punishable in connection with pornography was the manufacture, sale and/or distribution. Mere consumption was not illegal. But most countries have recently enacted legislation prohibiting possession of pornography depicting acts of violence. *In order to fight trafficking in human beings for the purpose of sexual exploitation through the use of new information technologies, countries should consider to review their legislation in order to penalise the production, distribution and possession of pornography depicting acts of violence.*

It would also be interesting to review regulations in the different national legislations *concerning criminal liability of the creator of a hyperlink* appearing on an Internet page for the content of the page to which the user is sent via this link, or of the moderators of chats, as these actors can have knowledge about the content of these sites or messages and could eventually provide access to sites related to, or to persons involved in, child pornography or trafficking for the purpose of sexual exploitation.

It might also be useful to consider *legislation aimed at regulating matrimonial agencies to avoid the abuse of such agencies in connection with trafficking for the purpose of sexual exploitation.* One possible direction might be to require strict formal conditions for the conclusion of such a contract. In particular, the conclusion of such a contract over the Internet should not be permitted. A requirement to notify the authorities

where the couple will live of the country of origin of the foreign potential spouse or partner might be a useful instrument.

As regards child pornography, in accordance with Recommendations No. R (2000) 11 and Rec (2001) 16, which propose that protection of children includes all boys and girls *up to the age of 18 in all countries*, states should make acts which constitute *sexual exploitation of children up to 18 criminal offences under their penal legislation.*

Because of the international dimension of the criminal offences in question the *double incrimination requirement can hinder effective prosecution*. One of the solutions would be for the government of a country to pass legislation to prosecute its own nationals for acts which constitute a crime under the law of such country regardless of where the acts were committed. *States should review all regulations which hinder the incrimination of persons who have committed crimes related to trafficking in human beings for the purpose of sexual exploitation.*

In the field of money laundering, criminal provisions formerly concerned only drugs and organised crime. The recent trend is for these provisions not to be subject to such limitations, but rather to have them apply to many, if not all, types of crimes including trafficking in persons for the purpose of sexual exploitation. *Member states should review their money laundering legislation in order to include all types of crimes including trafficking in human beings for the purpose of sexual exploitation through new information technologies.*

Most multilateral instruments on trafficking for the purpose of sexual exploitation were set up within a limited geographical area, confined to Europe. These instruments must reach beyond Europe if the appearance of "virtual havens" was to be prevented. *States should develop and encourage close co-operation at national and international level between the bodies working in the same field.*

At international level *there is no internationally approved instrument on the content circulating on the Internet for trafficking in human beings for the purpose of sexual exploitation. There is a need for common legislation, for co-operation agreements and for co-operation between countries at legal, technical and judicial level.*

As a first step, governments involved in the fight against cybercrime should be *encouraged to ratify the European convention on cybercrime of the Council of Europe.*

The transient and intangible nature of the Internet, as well as the anonymity and secrecy that communications via the Internet permits, make the identification of the author and/or intended recipient of an illicit communication, as well as the collection of evidence, much more difficult and elusive. *There is a need to pass legislation to adapt procedural and investigative tools to the specificities of the new technologies.*

Taking into consideration that communication networks – including the Internet – are frequently used to commit crimes, law enforcement authorities need to be able to use traffic data[1] for investigation and prosecution purposes.

Specific *training on investigating the Internet, as well as specific international procedures and agreements between national police authorities should be set* up or further developed in order to allow the police to intervene effectively against cybercriminality and to neutralise networks by international co-ordinated action.

Another problem with which the police authorities must increasingly contend is that messages are encrypted making them impossible to read. To give police the power to order decryption of messages will greatly enhance the ability to prosecute criminals in this domain. *Governments should develop special provisions allowing the police to obtain assistance from any expert in the field of encryption and give police enforcement agencies the necessary means and fundings to develop computer techniques and knowledges in order to fight cyber related crime.*

As far as messages sent through anonymers are concerned, law enforcement should be able to access anonymous remailer's database. *Measures should be taken in order to make anonymisers illegal to be required to retain client and connection information making it possible to identify the messages for communication to the authorities upon requisition by a judge in the context of a court inquiry. International co-operation should be developed in order to make these measures effective.*

One major concern is that in many countries entrapment is illegal. In the case of trafficking in human beings for the purpose of sexual exploitation in general, specific measures should be envisaged to give the police the means to identify the individuals violating the law on IRC channels.

Agreements on communication of information on illegal data on the network must be further improved between the authorities and Internet service providers. *Regulations should be adopted defining minimum data and how long they should be kept accessible for the authorities by access and service providers so that the source of material sent by the Internet can be identified.*

Transborder co-operation should also be developed in order to find solutions for data sent from "Internet havens", countries without legislation for prosecuting certain types of crime.

1. Information elements on the signal/data transmission needed to realise or to control the telecommunication; **does not include** the contents of the communication.

2. Protection of the victims and prevention

The question of victims should be considered as *a high priority* for the society and for the governments. As regards the protection of victims and witnesses, governments *should be encouraged to implement the measures provided for in Recommendation No. R (2000) 11 and Recommendation Rec (2001) 16* in particular, as regards the *consent of a person*. Because of the extremely poor living conditions in the countries from which these persons come, such consent is almost always given, but it should not be treated *as consent sufficient to prevent incrimination* of the perpetrators of trafficking in human beings for the purpose of sexual exploitation. They should be first regarded as victims. It should be noted that in the case of trafficking, the Protocol to Prevent, Suppress and Punish Trafficking for the purpose of sexual exploitation in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, does not take into account the consent of the person.

Preventive measures should first aim at effectively controlling the Internet:

- *reform of education and training systems* in order to give young people, judges, journalists, teachers, police forces, administrative departments and partners in the private sector tools that would enable them to learn how to use the new technologies and constantly adjust their knowledge;
- *raise awareness to increase self-regulation of all the parties involved* (authors, service providers, hosts, access providers, transporters, companies and individuals) and acceptation: this entailed raising all the players' awareness of the dangers of broadcasting illegal content on the Internet. Governments should encourage that codes of good conduct and self-regulating practices will be adopted, and that filtering systems and labelling procedures will be set up;
- the need to strengthen international co-operation.

Legal mechanisms should be developed in order to unable victims whose images are still on the web to get them withdrawn from the Web and to avoid that they become victims again.

Prevention should also focus on two aspects:

- *against victimisation* of women and/or children; and
- *against violent behaviour* of men and/or members of criminal organisations.

This second type of prevention focuses on education within families, schools, universities, media, etc. It is linked to the social climate and its impact on individuals and groups within our societies. Such distinctions are important to develop and implement more effective strategies.

Professionals, public authorities, organisations and civil society must be involved at their respective levels and work in co-operation in order to combat and prevent this phenomenon. Ad hoc measures should also be taken in order to give all the partners the means to better understand the problem:

- Research on trafficking in human beings for the purpose of sexual exploitation through the use of new technologies should be encouraged, as far as the evolution of demand and its consequences on trafficking for the purpose of sexual exploitation are concerned. This research should concern persons using NITs with a pornographic/sex-related motivation. There is also a lack of data and research to substantiate the assumptions of NGOs that women who find partners through marriage agencies are at higher risk of becoming victims of violence and exploitation.
- Public authorities should adapt their legislations to penalise the use of new technologies for trafficking for the purpose of sexual exploitation, set up and implement comprehensive policies to co-ordinate preventive measures in consultation with NGOs and experts; set up assistance programmes for the victims including therapies, employment opportunities, etc., support research in the field of prevention of trafficking for the purpose of sexual exploitation via the new information technologies and in the field of the prevention of violence;
- Law enforcement and judiciary should be trained on trafficking for the purpose of sexual exploitation via the new information technologies, in particular judges should be trained to understand the psychology of the victims and work in co-operation with NGOs and law enforcement; journalists should be trained in order to inform the public on trafficking for the purpose of sexual exploitation without sensationalism and to avoid stereotypes.
- NGOs should develop and implement assistance programmes for the victims, launch awareness campaigns against trafficking for the purpose of sexual exploitation and campaigns against stereotypes; the media and public authorities could help them to find "sponsors" to support them.

Research should be encouraged and supported to understand the whole complexity of the problem and its pro-active factors over the last decade and to raise awareness (mistakes committed for empowering criminals, non-reactions, good practices of NGOs). It would also be very important to have research developed on the users in order to understand the variety of motivations of the perpetrators and to develop preventive policies and strategies.

3. Combating harmful and illegal contents on the Internet and the freedom of expression

Recommendation Rec (2001) 8 sets forth the importance of developing a quality labelling system that assists users both to block content and to help find valuable content. The need to promote positive, high quality, independent content and educate users to find it is an essential part of the solution. *Governments and the private sector may consider creating financial incentives or sponsoring the development of technologies that promote Internet content in the public interest.*

Much information is available on the "abuse" of the Internet, but one does not know how to react or whom to contact. A number of official points of contact do exist and could serve as "clearing houses", but awareness-raising measures are needed to inform people about the possibilities at their disposal. For instance:

- a directory of useful sources at European level should be published;
- an Internet user guide for parents and children should be produced;
- a Web site with useful links should be created;
- the activities of NGOs which do work of this kind should be supported;
- the Belgian good practice of the European centre for missing children should be followed elsewhere;
- user-friendly telephone help lines ("freephone numbers") should be made available.

As regards the *content labelling issue*, a rational approach should be adopted, taking into account the requirements of the European Convention on Human Rights (ECHR), in particular Article 10 on freedom of expression and information. Labelling should be used only *for information purposes and in a neutral manner.*

Technical intermediaries should be liable for the illicit contents which they provide. The Directive of the European Union 2000/31/CE of June 8, 2000 provides that *they are totally exonerated from liability if they have knowledge of illegal content which they may store or transmit.* A *constructive dialogue should be fostered between them and the prosecutors*, as well as NGOs dedicated to monitoring illegal contents on the Net. They are ready to co-operate, especially to block access to illegal

websites. But it must be noted that the police does not agree with this approach as this kind of action can destroy the work to track the criminals on Internet. *Memorandums of agreement should be signed between NGOs and law enforcement in order to set-up co-operation and exchange information in this field.*

Finally, given the ease of the methods of payment on the Internet, public authorities should consider whether Companies involved in money transfers should be liable for knowingly co-operating with groups and/or individuals involved in trafficking in human beings for the purpose of sexual exploitation.

4. Raising awareness, information and the role of the media

Within media, standards of professionalism should be promoted that will assist journalists in addressing the ethical dilemmas they confront when reporting on trafficking in human beings for the purpose of sexual exploitation.

As regards the importance of the contribution the media could make to raising public awareness, professional organisations and networks need to assess their roles in education, advice, and raising awareness. *The mass media do not only have an awareness-raising role to play towards the public, but they can also stimulate public debate and provide an incentive to the adoption of political measures to combat this new form of crime.*

Also, a more vigilant advertising policy should be adopted by the media. While they cannot be made liable for the contents of classified advertisements, they could adopt a code of practice that requires them to reject those advertisements that are easily identified as aimed at luring women into prostitution.

Schools of journalism should include in their curricula education to human rights. Gender awareness should not merely be treated as a special topic, but infused into *all aspects* of journalist and media training. Journalists should also be trained in order to avoid *sensationalism and stereotypes* when reporting on cases of trafficking in human beings for the purpose of sexual exploitation.

There is a need for better co-operation between media, police and NGOs involved in the fight against trafficking in human beings for the purpose of sexual exploitation. Media in the countries of origin of the exploited women could work with police and organisations in civil society in providing women with information about the risks involved. In western Europe media has a role to play in making the general public and often the police understand that these women are *not criminals* but *victims* of *trafficking in human beings for the purpose of sexual exploitation.*

B. Recommendations

The experts recall that the Council of Europe has been working on the problem of trafficking in human beings for the purpose of sexual exploitation and those linked to cybercrime and that it has already adopted legal instruments in these fields: Recommendation No. R (2000) 11 on action against trafficking in human beings for the purpose of sexual exploitation, Recommendation Rec (2001) 16 on the protection of children against sexual exploitation, the Convention on cybercrime and Recommendation Rec (2002) 8 on self-regulation and user protection against illegal or harmful content on the new communications and information services are new European legal instruments which give tools and guidelines to the member states of the Council of Europe to better fight this phenomenon.

It is recommended that the member states implement these instruments and ratify the Convention on Cybercrime in order to fight effectively trafficking in human beings for the purpose of sexual exploitation and child pornography. The work undertaken for the drafting of these instruments and other European and international instruments dealing with the question of trafficking in human beings for the purpose of sexual exploitation and with the use of new technologies, as well as their report on the impact of the new information technologies on trafficking in human beings for the purpose of sexual exploitation should be taken into account when a European convention on the fight against trafficking in human beings is drafted.

Such a convention should be based on a human rights approach and protect the rights of women and children to be free of criminal acts of trafficking for the purpose of sexual exploitation, even through new information technologies. It should give priority to assisting and protecting victims from traffickers. In the framework of this convention, the question of trafficking for the purpose of sexual exploitation through new information technologies definition of trafficking should be considered with the aim to deal with the question of trafficking in images which are detrimental to real people.

The Council of Europe should gather and co-ordinate the information and expertise collected at national level on action against trafficking in human beings for the purpose of sexual exploitation and support the research in this field. A fundamental knowledge of the development of the problem and its proactive factors could help raise awareness and understand the whole complexity of the problem as well as the measures which should be taken.

The Council of Europe should also support initiatives that bring together media professionals, police and NGOs to create better co-operation in the fight against trafficking in human beings for the purpose of sexual exploitation.

Finally, the group of experts recommends that the Council of Europe should play a role in international co-ordination and encourage countries to pass legislation, sign agreements or adopt international procedures. Codes of conduct that exist in certain countries could serve as the basis for legislation or guidelines at European level, which could be prepared by experts within the Council of Europe.

Appendix 1. Terms of reference of the EG-S-NT

Specific terms of reference

1. Name of the committee

Group of Specialists on the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation (EG-S-NT).

2. Type of committee

Committee of experts.

3. Source of terms of reference

Steering Committee for Equality between Women and Men (CDEG).

4. Terms of reference

For the purpose of implementing the decisions of the 2nd Council of Europe Summit of Heads of State and Government (Strasbourg, October 1997) concerning new information technologies and the fight against all forms of sexual exploitation, the EG-S-NT shall address, under the authority of the CDEG, the impact of new information technologies on equality between women and men and in particular on trafficking in human beings for the purpose of sexual exploitation. Taking into account the work already undertaken by the CDEG in the area of trafficking in human beings for the purpose of sexual exploitation,[1] and in particular the work recently undertaken by its Multisectoral Group (EG-S-TS)[2] as well as that carried out by other national and international bodies,[3] the Group is instructed in particular to:

(i) consider in depth the scale of the impact of the use of new information technologies on trafficking in human beings for purposes of sexual exploitation, specifying:

- the techniques used and how they work;
- the various kinds of users and their motives;
- existing legislation in the member states and relevant international texts.

The resulting study should be based in particular on information (statistical or other) which the Group is responsible for collecting.

(ii) study the effects of the use of these new technologies on the victims of trafficking and the resulting violations of human rights, as well as the negative effects on some users;[4]

(iii) prepare, on this basis, guidelines for media professionals, the boards of newspapers and other press and audiovisual media, public authorities and non-governmental organisations and associations, as well as any other persons involved; these guidelines may be prepared inter alia on the basis of codes of conduct already available at national level.

---

1. I.e. the Seminar on Action against Traffic in Women and Forced Prostitution as Violations of Human Rights and Human Dignity (Strasbourg, 25 September 1991), the work of the Group of Specialists on Action against Traffic in Women and Forced Prostitution (EG-S-TP) (1992-93) and the Plan of Action prepared by Ms Michèle Hirsch (document EG (96) 2). See also the report of the meeting of chairs of Council of Europe steering and other committees (Strasbourg, 6 September 1996) (document CDEG-TP (96) 1) and the replies to the questionnaire sent to these committees.
   See also the conclusions of the Seminar on "Action against traffic in human beings for the purpose of sexual exploitation: the role of NGOs" (Strasbourg, 29-30 June 1998) and of the Workshop on "good" and bad practices regarding the image of women in the media (Strasbourg, 28-29 September 1998).
2. The Multisectoral Group on Action Against Trafficking in Human Beings for the purpose of sexual exploitation (EG-S-TS) started work in December 1997, under the authority of the CDEG, and has been entrusted with preparing a draft recommendation of the Committee of Ministers to member states.
3. European Union, United Nations, International Organisation for Migration, Budapest Group, INTERPOL, EUROPOL, etc.

5. Membership

The Group EG-S-NT is a multisectoral Group of Specialists comprising experts from three Council of Europe committees and headed by the CDEG. It has the following eight members, whose travel and subsistence expenses are defrayed by the Council of Europe:

a) one member of the CDEG (the Netherlands) and three experts appointed by it;
b) two experts appointed by the CDMM;
c) two experts appointed by the CDPC.

These experts will be appointed by the committees in consultation with the Secretariat, bearing in mind the need to ensure an equitable geographical distribution of seats.

One representative of the European Commission will be invited to attend the Group's meetings – without the right to vote or to have his/her expenses reimbursed by the Council of Europe.

Representatives from the International Organisation for Migration (IOM), Interpol, Europol, the Crime Prevention Commission of the United Nations, and the United States of America will also be invited to attend the Group's meetings – without the right to vote or to have their expenses reimbursed by the Council of Europe.

4. The use of new information technologies in the field of trafficking creates several kinds of victims. Internet is used by traffickers to "recruit" potential victims, but the following should also be mentioned: women/children who are directly abused through the production of videos; persons who have survived porn productions and become traumatised because of the new possibilities of Internet Relay Chat (IRC), the World Wide Web (WWW) and other tools (it becomes unbearable for them to imagine that their private documentation can be seen by millions of people all over the world); relatives of the victims who see these pictures while using Internet or WWW, etc.

6. Expert qualifications required

Specialists on questions concerning the development of new information technologies; a good knowledge of questions relating to access to these services and their regulation/self-regulation and/or questions relating to equality between women and men (trafficking in human beings/violence against women) is desirable.

7. Working methods

The Group shall elect its Chair and Vice-Chair for the duration of its terms of reference.

Within its terms of reference, the EG-S-NT may organise such contacts and consultations, including hearings, with interested professionals and others as it deems necessary for discharging its terms of reference.

8. Duration

The Group shall begin its work once its terms of reference have been approved by the Committee of Ministers and shall cease its activity on 31 December 2002.

Appendix 2. Members of the group of specialists EG-S-NT

Steering Committee for Equality between women and men
Comité Directeur pour l'Égalité entre les femmes et les hommes (CDEG)

Albania/Albanie

Ms Eglantina GJERMENI

University of Tirana
Rr. Q. Stafa, P.1
Shk. 1, Ap. 5
Tirana
Albania

Germany/Allemagne

Ms Monika GERSTENDÖRFER

Managing Director
Lobby für Menschenrechte e.V.
PO Box 10 30
D-72541 Metzingen
Germany

Lithuania/Lituanie

Mr Oleg SYSHCHIKOV

Police Department at the Ministry of Internal Affairs of the Republic of Lithuania
Organized Crime Investigation Service
19 Saltoniskiu str.
2034 Vilnius
Lithuania

Netherlands/Pays-Bas

Ms Flora VAN HOUWELINGEN

Deputy Director
Ministry of Social Affairs and Employment
Department for the Co-ordination of Emancipation Policy (DCE)
Postbus 90801
NL-2509 LV The Hague
The Netherlands

Steering Committee on the Mass Media
Comité Directeur sur les moyens de communication de masse (CDMM)

Iceland/Islande

Ms Sigrún STEFANSDÓTTIR

Informationschef
NMR/NR Store Strandstræde 18
DK-1255 Kobenhavn
Denmark

European Committee on Crime Problems
Comité européen sur les problèmes criminels (CDPC)

Belgium/Belgique

M. Roland WALRAET

Federal Computer Crime Unit
Rue du Noyer, 211
B-1000 Bruxelles
Belgium

Consultant expert
Experte consultante

Ms Donna HUGHES

Carlson Endowed Chair, Women's Studies
University of Rhode Island
316 Eleanor Roosevelt Hall, Suite 3
Kingston, Rhode Island 02881
United States

International organisations
Organisations internationales

Interpol

Mr Jan AUSTAD

2000, quai Charles de Gaulle
F-69006 Lyon
France

Appendix 3. International instruments

The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), adopted in 1979 by the United Nations General Assembly, defines what constitutes discrimination against women and sets up an agenda for national action to end such discrimination.

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, establishes a definition of trafficking for the purpose of sexual exploitation and regulations which should be considered as a starting point for any further initiative on the subject. The definition is the outcome of a long negotiation. It involves the countries of origin, of transit and destination of all the areas in the world, and covers all forms of trafficking for the purpose of sexual exploitation , except trafficking for the purpose of sexual exploitation through the new information technologies.

ILO Convention No. 182 on the worst forms of child labour (1999) identifies the elimination of the worst forms of child labour as the main priority for national and international action, including international co-operation and assistance. It might possibly be used in some cases of combating trafficking for the purpose of sexual exploitation where minors are involved.

The Framework Decision of the European Council on combating trafficking for the purpose of sexual exploitation in human beings focuses mainly on investigation and prosecution. Despite the fact that the Decision defines trafficking for the purpose of sexual exploitation in human beings as a serious violation of human rights and human dignity, the essential objective is to establish severe and dissuasive sanctions, to improve judicial co-operation and prevention of crime. In matters of victims' rights, the Decision states that member states should ensure that the victim "is given adequate legal protection and standing in judicial proceedings" and that "criminal investigations and judicial proceedings do not cause any additional damage for a victim".

Recommendation No. R (2000) 11 of the Committee of Ministers of the Council of Europe on action against trafficking for the purpose of sexual exploitation in human beings for the purpose of sexual exploitation. This recommendation was adopted in May 2000. It is the first text adopted by the Council of Europe on trafficking for the purpose of sexual exploitation in human beings, and the first one ever to establish a clear definition of trafficking for the purpose of sexual exploitation for the purposes of sexual exploitation, but which does not include any provision concerning trafficking for the purpose of sexual exploitation and the new information technologies. The negotiations of this definition constituted a very important basis for the work on the UN Protocol.

Recommendation Rec (2001) 16 of the Committee of Ministers of the Council of Europe on the protection of children against sexual exploitation. The drafters of this recommendation considered that pornography does not necessarily imply the use of a real child and that broadcasting images or virtual images is sufficient to constitute pornography as, even though there are no real people involved, the victim is denoted by the image of the person thus depicted.

The Convention on Cybercrime of the Council of Europe (2001) is the first binding international treaty on the subject. It deals, in particular, with offences related to copyright violations, computer related fraud, child pornography (Article 9) and offences connected with network security. It focuses specifically on the sexual exploitation of children in Article 9, which makes it a criminal offence not only to produce child pornography for distribution through a computer system, but also to offer this kind of pornography, to make it available, to distribute or transmit it, to procure it or to possess it in a computer system.

Appendix 4. State of signatures and ratifications of international instruments on action against trafficking[1]

1. Convention on the Elimination of All Forms of Discrimination against Women

Country	Signature	Ratification
Albania		11 May 1994
Andorra		15 January 1997
Armenia		13 September 1993
Austria	17 July 1980	31 March 1982
Azerbaijan		10 July 1995
Belgium	17 July 1980	10 July 1985
Bosnia-Herzegovina		01 September 1993
Bulgaria	17 July 1980	08 February 1982
Croatia		09 September 1992
Cyprus		23 July 1985
Czech Republic		22 February 1993
Denmark	17 July 1980	21 avril 1983
Estonia		21 October 1991
Finland	17 July 1980	04 September 1986
France	17 July 1980	14 December 1983
Georgia		26 October 1994
Germany	17 July 1980	10 July 1985
Greece	02 March 1982	07 June 1983
Hungary	06 June 1980	22 December 1980
Iceland	24 July 1980	18 June 1985
Ireland		23 December 1985
Italy	17 July 1980	10 June 1985
Latvia		14 avril 1992
Liechtenstein		22 December 1995
Lithuania		18 January 1994
Luxembourg	17 July 1980	02 February 1989
Malta		08 March 1991
Moldova		01 July 1994
Netherlands	17 July 1980	23 July 1991
Norway	17 July 1980	21 May 1981
Poland	29 May 1980	30 July 1980
Portugal	24 avril 1980	30 July 1980
Romania	04 September 1980	07 January 1982
Russian Federation	17 July 1980	23 January 1981
San Marino		
Serbie -Monténégro		12 March 2001
Slovakia		28 May 1993
Slovenia		06 July 1992
Spain	17 July 1980	05 January 1984
Sweden	07 March 1980	02 July 1980
Switzerland	23 January 1987	27 March 1997
The former Yugoslav Republic of Macedonia		18 January 1994
Turkey		20 December 1985
Ukraine	17 July 1980	12 March 1981
United Kingdom	22 July 1981	07 avril 1986

2. United Nations Convention against Transnational Organized Crime

Country	Signature	Ratification[a]
Albania	14 December 2000	21 August 2002
Andorra	11 November 2001	
Armenia	15 November 2001	01 July 2003
Austria	12 December 2000	
Azerbaijan	12 December 2000	
Belgium	12 December 2000	
Bosnia-Herzegovina	12 December 2000	24 avril 2002
Bulgaria	13 December 2000	05 December 2001
Croatia	12 December 2000	24 January 2003
Cyprus	12 December 2000	22 avril 2003
Czech Republic	12 December 2000	
Denmark	12 December 2000	
Estonia	14 December 2000	10 February 2003
Finland	12 December 2000	
France	12 December 2000	29 October 2002
Georgia	13 December 2000	
Germany	12 December 2000	
Greece	13 December 2000	
Hungary	14 December 2000	
Iceland	13 December 2000	
Ireland	13 December 2000	
Italy	12 December 2000	
Latvia	13 December 2000	07 December 2001
Liechtenstein	12 December 2000	
Lithuania	13 December 2000	09 May 2002
Luxembourg	13 December 2000	
Malta	14 December 2000	
Moldova	14 December 2000	
Netherlands	12 December 2000	
Norway	13 December 2000	
Poland	12 December 2000	12 November 2001
Portugal	12 December 2000	
Romania	14 December 2000	04 December 2002
Russian Federation	12 December 2000	
San Marino	14 December 2000	
Serbia and Montenegro	12 December 2000	06 September 2001
Slovakia	14 December 2000	
Slovenia	12 December 2000	
Spain	13 December 2000	01 March 2002
Sweden	12 December 2000	
Switzerland	12 December 2000	
The former Yugoslav Republic of Macedonia	12 December 2000	
Turkey	13 December 2000	25 March 2003
Ukraine	12 December 2000	
United Kingdom	14 December 2000	

a. The convention entered into force on 29 September 2003.

1. Updated: September 2003.

3. Protocol to prevent, suppress and punish trafficking in persons, especially women and children, supplementing the United Nations Convention against Transnational Organized crime

Country	Signature	Ratification
Albania	12 December 2000	21 August 2002
Andorra	12 December 2000	
Armenia	15 November 2001	01 July 2003
Austria	12 December 2000	
Azerbaijan	12 December 2000	
Belgium	12 December 2000	
Bosnia-Herzegovina	12 December 2000	24 avril 2002
Bulgaria	13 December 2000	05 December 2001
Croatia	12 December 2000	24 January 2003
Cyprus	12 December 2000	06 August 2003
Czech Republic	10 December 2002	
Denmark	12 December 2000	
Estonia	20 September 2000	
Finland	12 December 2000	
France	12 December 2000	29 October 2002
Georgia	13 December 2000	
Germany	12 December 2000	
Greece	13 December 2000	
Hungary	14 December 2000	
Iceland	13 December 2000	
Ireland	13 December 2000	
Italy	12 December 2000	
Latvia	10 December 2002	
Liechtenstein	14 March 2000	
Lithuania	25 avril 2002	23 June 2003
Luxembourg	13 December 2000	
Malta	14 December 2000	
Moldova	14 December 2000	
Netherlands	12 December 2000	
Norway	13 December 2000	
Poland	04 October 2001	
Portugal	12 December 2000	
Romania	14 December 2000	04 December 2002
Russian Federation	12 December 2000	
San Marino	14 December 2000	
Serbia and Montenegro		
Slovakia	15 November 2001	
Slovenia	15 November 2001	
Spain	13 December 2000	01 March 2002
Sweden	12 December 2000	
Switzerland	02 avril 2002	
The former Yugoslav Republic of Macedonia	12 December 2000	
Turkey	13 December 2000	25 March 2003
Ukraine	15 November 2001	
United Kingdom	14 December 2000	

4. ILO Convention No. 182 concerning the prohibition and immediate action for the elimination of the worst forms of child labour

Country	Signature	Ratification
Albania		02 August 2001
Andorra		
Armenia		
Austria		04 December 2001
Azerbaijan		
Belgium		08 May 2002
Bosnia-Herzegovina		05 October 2001
Bulgaria		28 July 2000
Croatia		17 July 2001
Cyprus		27 November 2000
Czech Republic		19 June 2001
Denmark		14 August 2000
Estonia		24 September 2001
Finland		17 January 2000
France		11 September 2001
Georgia		24 July 2002
Germany		18 avril 2002
Greece		06 November 2001
Hungary		20 avril 2000
Iceland		29 May 2000
Ireland		20 December 1999
Italy		07 June 2000
Latvia		
Liechtenstein		
Lithuania		
Luxembourg		21 March 2001
Malta		15 June 2001
Moldova		14 June 2002
Netherlands		14 February 2002
Norway		21 December 2001
Poland		09 August 2002
Portugal		15 June 2000
Romania		13 December 2000
Russian Federation		
San Marino		15 March 2000
Serbia and Montenegro		
Slovakia		20 December 1999
Slovenia		08 May 2001
Spain		02 avril 2001
Sweden		13 June 2001
Switzerland		28 June 2000
The former Yugoslav Republic of Macedonia		30 May 2002
Turkey		02 August 2001
Ukraine		14 December 2000
United Kingdom		22 March 2000

5. European Convention on Cybercrime

Country	Signature	Ratification
Albania	23 November 2001	20 June 2002
Andorra		
Armenia	23 November 2001	
Austria	23 November 2001	
Azerbaijan		
Belgium	23 November 2001	
Bosnia-Herzegovina		
Bulgaria	23 November 2001	
Croatia	23 November 2001	17 October 2002
Cyprus	23 November 2001	
Czech Republic	23 November 2001	
Denmark		
Estonia	23 November 2001	12 May 2003
Finland	23 November 2001	
France	23 November 2001	
Georgia		
Germany	23 November 2001	
Greece	23 November 2001	
Hungary	23 November 2001	
Iceland	30 November 2001	
Ireland	28 February 2002	
Italy	23 November 2001	
Latvia		
Liechtenstein		
Lithuania		
Luxembourg		
Malta	17 January 2002	
Moldova	23 November 2001	
Netherlands	23 November 2001	
Norway	23 November 2001	
Poland	23 November 2001	
Portugal	23 November 2001	
Romania	23 November 2001	
Russian Federation		
San Marino		
Serbia and Montenegro		
Slovakia		
Slovenia	24 July 2002	
Spain	23 November 2001	
Sweden	23 November 2001	
Switzerland	23 November 2001	
The former Yugoslav Republic of Macedonia	23 November 2001	
Turkey		
Ukraine	23 November 2001	
United Kingdom	23 November 2001	

Appendix 5. The Yahoo! case

LICRA and UEJF v. Yahoo! Inc. and Yahoo! France. Order of 20 November 2000 by the Superior Court of Paris[1]

by **Judge Jean-Jacques GOMEZ**, First Deputy Chief Justice of the Superior Court of Paris,
rendered in public at the hearing held in summary proceedings, by delegation from the Chief Justice,
assisted by **Nicole VOURIOT,** Clerk of the Court

Plaintiffs

La Ligue contre le racisme et l'antisémitisme - LICRA,
represented by its President, Mr Patrick GAUBERT
42 rue du Louvre
75002 Paris
represented by Maître Marc LEVY,
barrister before the Bar of Paris, P 0119

The association Union des étudiants juifs de France (UEJF),
acting through its President Mr Ygal LE HARRAR
27 ter, avenue Löwendal
75015 Paris
represented by Maître Stéphane LILTI,
barrister before the Bar of Paris, C1133

Defendants

Yahoo! Inc.
3420 Central Expressway
Santa Clara
California 95051
United States of America
represented by Maître Christophe PECNARD,
barrister before the bar of Paris, L0237

Société Yahoo! France
8 rue du Sentier
75002 Paris
represented by Maître Isabelle CAMUS,
barrister before the Bar of Paris, L0237

Voluntary intervenor

Le Mouvement contre le Racisme et pour l'Amitié entre les Peuples - MRAP
89 rue Oberkampf
75011 Paris
represented by Maître Didier SEBAN,
barrister before the bar of Paris, E0057

Present

Mr Public Prosecutor before the Superior Court of Paris
4 boulevard du Palais
75001 Paris
represented by Mr Pierre DILLANGE, First Substitute

1. **Unofficial English translation**. This English version of a French opinion was translated by Lapres & Associés in Paris.

We, the Chief Justice,

In the light of our order of May 22, 2000 to which we make expressly make reference and according to which we ordered

1. **Yahoo! Inc.** to take all measures such as would dissuade and render impossible all consultations on yahoo.com of the service of auctioning of Nazi objects as well as any other site or service which constitute an apology of nazism or which contest the nazi crimes;
2. and **Yahoo! France** to issue to all internauts, even before the latter were to use a link making it possible to pursue the search on yahoo.com a message informing such internauts of the risks to which they would be exposed if they pursued their search on such sites;
3. the pursuit of the present proceedings in order to enable Yahoo! Inc to submit for discussion by the parties the measures which it intends to take to end the nuisance and harm suffered as well as to prevent any future nuisances;

In the light of our order of 11 August 2000 included herein by reference as regards the facts and the arguments and claims of the parties;

In the light of the arguments presented by **LICRA** and **UEJE**, **MRAP** and reiterated at the hearing of 6 November 2000, which sought the objectives already presented in our priori order;

In the light of the arguments developed in their defence by Yahoo! France and by Yahoo! Inc. and which make the same claims as those presented in our prior order;

In the light of the report of the experts **Wallon, Vinton Cerf** and **Laurie**;

In the light of the memoranda submitted at the hearing and to which reference is expressly made;

After hearing the Prosecutor's oral arguments;

In the light of the documents submitted in evidence;

After having taking the oath of expert of Mr Vinton Cerf, an expert whose name is not included on any list, Mr Nortek, expert enrolled on a list but whose intervention in this instance is to translate the English in conjunction with Mrs Kinder, expert enrolled on a list of experts in such matters;

As regards the claims against Yahoo! Inc.

Whereas Yahoo! Inc. argues:

- our court is not competent to hear this dispute;
- there is no way technically to satisfy the terms of the order of May 22, 2000;
- were such means to exist, their implementation would entail such an increase in costs for the company, that it might even put its existence in jeopardy and would in some way compromise the existence of the Internet network, a space of freedom; which ill-accommodates attempts at control and restrictions on access;

Whereas in support of such arguments of incompetence, reiterated for the third time, Yahoo! Inc. argues that:

- its services are destined essentially to internauts located on the territory of the United States of America;
- its servers are located on the same territory;
- a coercitive measure against it could not be applied in the United States because this would contravene the first amendment of the Constitution of the United States which guarantees to all citizens freedom of speech and of expression;

Whereas, while it may be accurate that the site "Yahoo! Auctions" in general is intended principally to internauts based in the United States given the nature of the objects put on sale, to the methods of payment provided, to the terms of delivery, to the language and to the currency used, the same are not true of the sites auctioning objects representing symbols of the Nazi ideology which might interest and are accessible to any person who wishes to go to them, including French people;

Whereas**,** moreover, and as has already been ruled, the mere visualisation in France of such objects constitutes a violation of Article R-6456 of the Penal Code and therefore constitutes a nuisance to internal public order;

Whereas moreover, such visualisation obviously causes grief in France to the plaintiff associations who are justified in seeking its cessation and reparation;

Whereas also, Yahoo! says that it aims at a French audience since in response to a connection to its auction site from a computer located in France it responds by dispatching advertising banners in French;

Therefore the links of attachment in this case with France are sufficiently established, such as to make our court perfectly competent to hear the claim;

That the eventual difficulties of execution of our decision on the territory of the United States, invoked by Yahoo! Inc., cannot of themselves justify in and of themselves a preliminary objection based on lack of competence of the court;

That this argument will therefore be rejected;

Whereas, with respect to the argument developed by Yahoo! and which is based on the impossibility of implementing the technical means such as would satisfy the terms of the order of 22 May 2000, it is opportune first to cite the conclusions of the panel of experts which appear on pages 62 to 76 of their report;

Opinion of the experts

Preamble

The undersigned experts wish to emphasise that their role has been limited to answering the technical questions asked by the Court. In no way, their answers should be considered as a support, whether technical or moral, for the decisions of the court or, *a contrario*, as a criticism thereof.

The context

On 22 May 2000, Yahoo! France and Yahoo! Inc. were found liable by the Superior Court of Paris in the following terms:

"[The Court] Orders Yahoo! Inc. to take such measures as will dissuade and render impossible any and all consultation on yahoo.com of the auction service for Nazi objects as well as any other site or service which makes apologies of Nazism or questions of the existence of Nazi crimes;

Orders Yahoo! France to warn any and all surfers consulting yahoo.fr, and the foregoing prior to use of the link enabling him to pursue his search on yahoo.com where the result of his search, whether via the arborescence or through the use of key words, leads him to sites, pages or forums the title and/or contents of which constitute a violation of French law, as well for consultations of sites which display apologies of Nazism and/or exhibit uniforms, insignia, emblems reminiscent of those

which were worn or exhibited by the Nazis, or offering for sale objects or works the sale of which is strictly forbidden in France, it must interrupt the consultation of the relevant site lest it incur the sanctions stipulated by French law or answer to actions initiated against it;

Yahoo! France has stated that it has executed this decision. Yahoo! Inc. has argued that there does not exist a technical solution enabling it to fully respect the Court's ruling.

A panel of experts was then appointed to enlighten the Court with respect to the various technical solutions which might be implemented by Yahoo! Inc. with a view to executing the decision of 22 May.

Internet

The Internet is a combination of several hundred millions of computer networks and associated sites which are interconnected throughout the world. Routers are computers used for interconnecting these networks. It is estimated that there are one hundred million portable computers, desk computers, organisers, mobile telephones, etc.

A body of procedures was defined from 1973 to 1980, under the authority of the research laboratories of the American Army, (DARPA). These procedures, known under the name TCP/IP, are the heart of several hundred million protocols used on the Internet.

At the end of the 1980s CERN conceived the Web (WWW) which exploits complementary procedures, the http protocols and the HTML language, to implement this system of global sharing of information.

The applications which are the most prevalent are electronic mail (e-mail), forums (newsgroups), chat rooms, auction sales, telephony, video and radio on-line and many other services.

A common misunderstanding consists in saying that Internet services are provided by the Web. In fact, the Web is just one of the facets of the Internet.

Internet, which began as an experimental project used and developed by computer science researchers, has within ten years become a world-wide commercial enterprise. Internet service providers (ISPs) have built and exploited networks open to the public. The private networks of universities, of firms, and even home computers are interconnected by suppliers of internet service within a global network. Certain service providers have specialized in the supply of access to users of the telephone interconnections. Others are specialised in the supply of access to used of television by cable, to users of ISDN lines, to users of ADSL, local loops, etc. These providers are generally called Internet Access Providers. They generally offer different portal services, electronic mail, information, etc.

Each unit connected to the internet must have an IP address. At the outset, certain organisations had obtained stocks of addresses from MANA. These stocks were divided into sub-groups attributed to their customers. These addresses might be fixed for the units connected permanently or temporarily for users of the telephone commuted network, or mobile units (portable computers). These addresses are comprised of 32 bits structured in two parts. The network part and the individual part. WAP telephones do not each have an IP address. The WAP protocol uses a bridge to convert the WAP address into an IP address and vice versa.

IP addresses are represented by four series of octets converted into decimal numbers from 0 to 255.

This representation is not very convenient and so a system has been created for associating a name with an address. These names, which each correspond to an address, are called domain names. The conversion of a domain name into an IP numerical address is achieved in within a body of data distributed over the Internet (DNS). These DNS servers proceed by arborescence and are specialised according to the nature of the services provided (.com, .org, .edu, .gov, etc.) and according to countries (.fr, .uk, .sf, etc.).

But it must be understood that there is no rule of correspondence between the countries in domain names and the numerical IP address. For example, www.yahoo.fr does not correspond to an IP address of the French network.

Consequently, the extension of the domain name does not make it possible to determine to which network the IP numerical address belongs.

On the other hand, the allocation, originally carried out by MANA, then by ICANN, of IP addresses to internet service providers (ISPs) follows an arborescence which goes from, for example, the principal network, to a sub-network, to an access provider then to a local user.

It is possible to go backward from a determined IP address to an access provider, to a sub-network and to a principal network.

Therefore, certain organisations and certain service providers maintain databases which make it possible to find the co-ordinates of a network, of a sub-network, of a router or of a site from its IP address.

The DNS system offers access providers, to sites, etc., the possibility of registering with their co-ordinates their geographical location in the form of latitude and longitude. This is not an obligation.

The exploitation of the geographical locations of IP address holders is nevertheless of great interest, not only to aim advertising but also to ensure that the web develops harmoniously. Several service providers have available the technology and the databases which make it possible to geographical identify such and such an address whether fixed or even allocated dynamically. Several among them have introduced themselves to the Court's panel of experts to maintain that they had available the technical means making it possible for Yahoo! Inc. to execute the obligations imposed upon it by the Court.

The problem

To respect the terms of the ruling finding it liable and prohibiting access to auction sales of Nazi objects, Yahoo! must:

1. identify the geographical original and nationality of internauts seeking access to its auction site;
2. prevent French internauts or those connected from French territory from learning of the description of Nazi objects being auctioned and *a fortiori* from bidding.

On the geographical origin and nationality

The general case

The interrogation of a Web site by the public consists in putting into relation a user's work station (personal computer or other) with an intended site.

This operation involves the intervention of different categories of intermediaries: the supplier of access, the routers, one or more intended sites.

It is opportune at this stage to recall that the user's work station, the access supplier, the routers and intended sites are iden-

tified on the network by an address conform with the internet protocol (IP).

Whereas IP addresses of access suppliers, of routers and of intended sites are fixed, in the sense that there is a permanent bi-univocal link between and IP address and its holder, this is not the case for the address attributed to the work station of the user. This address is dynamically attributed, in a non-permanent manner, by the access supplier at the time of the connection.

But the access providers may only attribute IP addresses which have been allocated to them by the Net authorities. Such addresses follow an arborescence as was said above. The microcomputer of the internaut is given an IP address attributed to a supplier of access which belongs to a sub-network, which belongs to a network.

The panel of experts questioned the AFA, the association of internet access and service providers, to learn what fraction of internet connections carried out by access providers which do not provide IP addresses which are identifiable as French.

The answer was 20.57% as of 30 September 2000.

The panel also asked the AFA to what extent its adherents were representative of access providers operating on French territory.

The answer, according to a Médiamétrie study of March 2000, is "87% of internauts connecting from their homes use an access provider which is a member of the AFA".

It may be added that for reasons of telephone costs, French internauts mainly use the services of access suppliers which are present in their country.

It may therefore be estimated that almost 70% of the IP addresses attributed to French internauts may be associated with certainty to a French domiciliation of the access provider and be filtered.

This indeed is the fact which makes it possible for Yahoo! Inc. to post franco-french advertising banners on its auction sales site.

Annex B of this report shows the path of the connection of an internaut to the site of destination via the access provider Club-Internet (Grolier) using the PING and WHOIS functions of the Internet.

The exceptions

There are numerous exceptions.

A large number, of the order of 20%, arises from the multinational character of the access provider or the fact that it uses the services of an international ISP or private communications network.

The case of AOL is in this respect significant. AOL uses the services of the UUNET network. Dynamic IP addresses attributed by AOL appear as being localised in Virginia, where the headquarters of UUNET are located.

Therefore, the workstations of users residing on French territory appear on the Web as not being located on French territory.

The same applies to several private networks of large corporations (intranets) where the real addresses are encapsulated and carried in such a manner that the address given for the Internet site is that of the end of the tunnel.

Other exceptions arise from the desire of certain users to conceal their actual address on the web. Thus, there have arisen anonymisation sites, the purpose of which is to replace the actual IP address of a user with another address. In such cases it is not possible to know the geographical location of the customer of the access provider since its address may not be known. The only localisation known would be that of the anonymisation site but this is of no interest in the matter at hand.

Examination of the solutions proposed by the specialists in the trade

All the solutions proposed rested on an exploitation of the geographical information of the sites which have one or more permanent addresses. These bases are constituted for part from information obtained from DNS servers and for part from information gathered by the providers themselves.

Infosplit

The experts were able to observe that Infosplit was incapable of geographically locating the users of AOL France, the server of which was located in the United States, for the reasons evoked above.

NetGeo

Relying upon principles similar to those of Infosplit, this system is also incapable of localising internauts using a network for which the access provider attributes dynamic IP addresses which do not correspond to the actual geographical location of the user.

CyberLocator

This solution relies upon the exploitation of the geographical data obtained from the system of localisation by satellite (GPS).

It is totally inappropriate in the case at hand since rare are the internauts who have a GPS peripheral coupled to their workstations.

Internauts' declarations on their honour with respect to their nationality

Since, because of the exceptions cited above, no technique for filtering makes it possible to identify all French internauts or those connected from French territory, the panel of experts has considered the opportunity of having internauts subscribe a declaration on their honor as to their nationality.

Such a declaration might be subscribed upon the first connection to the site in dispute, in this case, the Yahoo! auction sales site, by an internaut whose IP address belongs to one of the exceptional régimes mentioned above.

A message (a cookie) placed on the workstation of the internaut would enable the internaut to avoid having to renew his declaration at the time of each connection.

Exploitation of nationality by Yahoo! Inc.

This is the second part of the problem. What to do once the nationality or localisation of the workstation are known?

The measures to be implemented depend on the facts of each case. They may not be generalised to all sites and services on the Net.

In the case at hand, the site to be taken into consideration is pages.auctions.yahoo.com. It is hosted by GeoCities, IP address 216.115.104.70, localisation 37°352 North, 121°956 West, GeoCities network registered by Yahoo!, 3400 Central Expressway, Suite 201, Santa Clara, CA 95051.

This site is a site for the sale by auction of miscellaneous objects and not just Nazi objects. The characteristic of this type of site is to enable the internaut to find easily the objects he is looking for.

It seems that in order to respect the terms of the decision of 22 May 2000, Yahoo! must not allow internauts of French nationality or calling from French territory to access such objects.

If, at the end of a search carried out by a request sent by a French internaut, one or more Nazi objects described as Nazi objects by their owner have been selected by the search engine, they must be hidden from the internaut and excluded from his search results.

But, obviously, it is not possible for Yahoo! to exclude *a priori* the objects which might not have been described by their owners as being of Nazi origin or as originating from the Nazi period, or the characteristics of which might not have been brought to the attention of Yahoo.

The verifications carried out by the panel of experts have confirmed that numerous Nazi objects were indeed presented as such by their owners.

A more radical solution is also possible. It would suffice that the search engine not execute requests including the word *Nazi* and which emanate from internauts recognised as French or declared as such.

The claim against Yahoo! Inc.

> "To describe the information carried by the net which makes it possible to determine the geographical origin of calls."

The Internet protocol (IP) associates the IP address of the transmitter and that of the intended party with each packet of information transmitted. The intended party is thus capable of knowing the IP address of the transmitter. There are three classes of IP addresses (A, B and C) a description of which is included in Annex P.

The first part of this address makes it possible to identify the network and the sub-network to which belong the access provide of the transmitter. These networks may be either national or multinational.

According to the Association française des fournisseurs d'accès (AFA), we may consider that 80% of the addresses which are attributed dynamically by the members of this association are identified as French. *A contrario*, 20% are not.

Among the information carried over the net, only the IP addresses of the transmitters make it possible to determine the geographical origin of the calls. 80% of the addresses attributed dynamically by access providers which are members of the AFA may be identified as being French.

But it needs to be pointed out that the geographical origin of which notice is taken is that of the site of the access supplier called by the internaut. Nothing prohibits a user from calling from France, by telephone, to an access supplier the telephone number of which is of foreign origin. In this event, the IP address attributed dynamically will most likely be identified as foreign. It is also possible for a foreigner to call an access provider located in France and to have himself attributed a French IP address.

However, we may estimate, in the present state of affairs, that more than 70% of IP addresses located on French territory may be identified as French.

The experts emphasise that nothing justifies the conclusion that it will remain this way in the future. Encapsulation is developing, service and access providers are going international and internauts are more and more looking for ways to protect their privacy.

> "To state if other information, originating in particular from telephone operators or cable operators, may be exploited both by access providers as well as servers domiciling the target sites to determine the origin of calls and, in such case, to describe them."

This is information carried by the operators of telecommunications services and cable-operators, but not carried over the internet. Therefore, the intended sites may not be identified.

French telecommunications operators systematically transmit the telephone number of the caller to the terminal of the person called. This information is not exploited in real time by the access provider. It is retained temporarily in a file for future searches. It is thus possible to know, *a posteriori*, after analysis of the history of the connections, what was at any one time the number of the caller to whom was attributed such and such an IP address or vice versa.

Cable-operators may also, upon request but *a posteriori*, associate an IP address, which they have at a given moment associated with the local site of their customer.

> "To describe the filtering procedures which may be implemented by Yahoo! to prohibit access to internauts operating from French territory to the sections which might be considered illicit by the French judicial authorities;
>
> In the event that no technical solution might guarantee a filtering at 100% reliability, to supply all technical elements and elements of fact which make it possible to appreciate the extent of filtering likely to be obtained for each of the procedures of filtering described by the consultants.
>
> More generally to provide all technical elements and elements of fact making it possible for the court to cause to be respected the access restrictions order against Yahoo! Inc."

The experts considered that for a technical solution to be effective, it must be adapted to the case at hand. The Yahoo! companies exploit a number of services (annex G) on the net, from personal pages (GeoCities) to astrology (Yahoo! astrology) including finance, etc. Most of these sites do not appear to be concerned by this dispute.

The decisions of the Court and the claims do not describe with precision only the auction sales site. No claim is made against other sites and services of Yahoo! with sufficient precision to enable the experts to propose technical solutions which are adapted and functional.

The experts limited therefore, in the present state, their answers to the case of auction sales (Yahoo! auctions).

They also excluded the examination of other technical measures which might be imposed upon third parties, not party to these proceedings. Neither the case of Proxy servers, nor the parametering of navigators of internauts are included in the mission conferred upon them by the Court.

Reply of the experts Laurie and Walton

These experts note that, in the present state of development of the Internet:

1. The numbers supplied by the AFA, cross-referenced with their personal experience, justify these experts in thinking that 70% of the IP addresses of French citizens or residents on French territory which may be correctly identified by specialised service providers such as Info-Split, GeoNet or others, using specialised databases.

2. Yahoo! Carries out a posting of advertising banners targeting internauts which the company thinks are French and that it has available the technical means enabling it to identify them.
3. Approximately 30% of the IP addresses attributed to French people may not be correctly identified using the above mentioned techniques.
4. Numerous sites, most often relating to national defense (cryptography), do not authorise access to certain pages of the site or to downloading of software until a declaration of nationality has been obtained from the internaut.
5. "Cookies" are in general use and make it possible to avoid having to retype certain information at each visit to a site. Anyone trying to destroy a cookie or to prevent its registering knows perfectly well that his consultations will be longer on the sites which transmitted them.
6. The Nazi objects are generally described as such by the sellers using the word *Nazi* in the description of the object, which appears as a sales argument.

Therefore, these experts consider that in addition to the geographical identification already practiced by Yahoo! to target its advertising, it would be appropriate to oblige internauts whose IIP address is ambiguous to subscribe a declaration of nationality.

This declaration on one's honour would apply only to internauts the IP address of whom could not be identified as being associated with a French ISP (for example, multinational ISPs such as AOL, an address emanating from an anonymiser or an encapsulation in a an address attributed by an intranet server).

This declaration might, at the discretion of Yahoo!, be subscribed either on the home page of its auction sales site, or only in the event of a search for Nazi items; if the word *Nazi* appears in the user's search, just before the processing of the search by the search engine.

In such circumstances, these experts consider that one cannot reasonably maintain that this would have negative effects on the performance levels and the response times of the server hosting the Yahoo! auction sales site.

The association of the two procedures, geographical identification of the IP address and declarations of nationality, would probably make it possible to reach a rate of filtering close to 90%.

Reply of the expert Vinton Cerf

We reproduce below in his own words the dissenting part of the opinion of the expert Vinton Cerf:

"It has been proposed that users identify where they are at the request of the web server, such as the one(s) serving yahoo.fr or yahoo.com. There are several potential problems with this approach. For one thing, users can choose to lie about their locations. For another, every user of the web site would have to be asked to identify his or her location since the web server would have no way to determine a priori whether the user is French or is using the Internet from a French location. Some users consider such questions to be an invasion of privacy. While I am not completely acquainted with privacy provisions in the European Union, it might be considered a violation of the rights of privacy of European users, including French users, to request this information. Of course if this information is required solely because of the French Court Order, one might wonder on what grounds all other users all over the world are required to comply.

Another complaint about the idea of asking user for their location in that this might have to be done repeatedly by each web site that the user accesses – yahoo cannot force every web site to make this request. When a user first contacts the server(s) at yahoo.fr or yahoo.com, one might imagine that the question of geographic location might be asked and then a piece of data called a cookie might be stored on the user's computer disk. Repeated visits to Yahoo sites might then refer to this cookie for user location information. The problem with this idea is that cookies are considered by many to be an invasion of privacy also, as a result many users either configure browsers to reject storage of cookies on their disk drives or they clear them away after each session on the Internet – thus forcing the query about geographical location each time the user encounters a Yahoo-controlled web site. Again, Yahoo would have no way to force a web site net under its control to either ask the location question or to request a copy of the cookie containing the location. Indeed, it would open up a vulnerability for each user if arbitrary web sites were told how to retrieve the cookie placed there by the Yahoo sites.

It has been suggested that the filtering need only apply to users accessing the Internet from French Territories or by users who are French citizens. It is not clear whether the jurisdiction of the French Court extends to actions taken by French citizens who are not in French territory at the time of their access to Internet.

For these and many other reasons, it does not appear to be very feasible to rely on discovering the geographic location of users for purposes of imposing filtering of the kind described in the Court Order."

***

Whereas it appears from the arguments that physical localisation of an internaut is possible on the basis of the IP address;

Whereas Yahoo! Inc. attempts to render these conclusions totally inapplicable by opposing the contents of a separate note of the of the experts, Mr Vinton Cerf;

But whereas first of all at the hearings devoted among others to testimony of the consultants, Mr Vinton Cerf, admitted the feasibility of such geographical localisation in the terms and conditions of the report and in the proportions which are indicated in the report, of which he approved the contents;

Whereas, moreover, his separate note of 5 November 2000, of which Yahoo! invites us to take note, does not contradict the conclusions of the report; that it contents itself to expose on the one hand that it would be "incorrect, in any case such as to induce in error", to affirm that it would be possible to determine with great reliability the physical localisation of an IP address, the terms "great reliability" being taken to mean, apparently, a degree of reliability far above the degree retained by the report which is of the order of 70% and on the other hand that the panel of experts ahs also admitted in its entirety that the reply which had been provided on this point could only relate to the

auction site selling nazi objects and that it could not be the object of extrapolations to sites and services under the control of Yahoo!;

Whereas it is opportune to recall moreover that Yahoo! Inc. has already implemented geographical localisation of French internauts and those operating from French territory who visit its auction site since it systematically posts advertising banners in French to the attention of such internauts which it has the means to locate; that Yahoo! Inc. may not validly sustain that the technology to be implemented in this case would be "crude" without any reliability, unless it were to be supposed that Yahoo! had decided to spend money to lose it or to trick its advertisers on the quality of the services and performance to which it had committed itself , which does not seem to be the case here;

Whereas, in addition to the geographical identification which it has already been showed is used by Yahoo! Inc. the report of the experts suggests that there be subscribed by those internauts the IP address of whom is ambiguous (transition through an anonymiser (site which guarantees anonymity) – or attribution of IP addresses by AOL Compuserve which do not take account of the country of origin of the subscriber) a declaration of nationality, in reality a declaration with respect to the geographical origin of the internaut, that Yahoo! Inc. might require either at the moment of the consultation of the home page, in the case of a search for Nazi objects, if the word *Nazi* appears in the request of the user, just before the treatment of the request by the search engine;

Whereas the experts, who contest the allegations of Yahoo! Inc. with respect to the negative effects of such a control on the performance levels and the response time of the server hosting the auction sale site, estimate that the association of the two procedures, geographical identification and declaration of nationality make it possible to achieve a rate of filtering close to 90%;

Whereas, as regards the optimisation of the filtering by association of key words, the experts were of the opinion during the hearings that it would no doubt be necessary in order to optimize this filtering to select some ten words associated with search engines of documents or used for searching chains of characters "and" "or" "except";

Whereas in addition to the measures suggested by the experts, it is appropriate to add the controls by Yahoo! of the place of delivery of objects acquired by auction;

Whereas, in effect, a visit to a site for auctioning Nazi objects is not just for the purpose of looking; that its purpose is often the purchase of objects, therefore, if Yahoo! has not been able to identify with certainty the geographical origin, in the case at hand French, of the internaut, it will be aware of the place of delivery, and be able to prevent the delivery when same is programmed to be France;

Whereas, moreover, based on the linguistic version of the navigator, Yahoo! Inc. might have available additional information on the nationality of the internaut;

Whereas it might nevertheless sustain that the use of such information would require that it modify the software it uses to manage its sites and a notable increase in the associated material resources;

That it adds that the filtering of all information at the level of the web server could only be implemented if it were possible to know that the prohibition would apply only to French internauts, lest internauts from the rest of the world be prevented from accessing the information published on such sites, which is not imaginable;

But whereas, first of all, it has been demonstrated that it has the technical operational means to carry out filtering;

Whereas, moreover, it has not demonstrated with a convincing projection, that the technical adaptation made necessary to control the access to the Nazi objects auction site would entail a significant increase of the associated material resources;

Whereas, in any case, Yahoo! Inc. has offered to cooperate with the plaintiffs; therefore, it has requested that notice be taken that it is willing to implement a system of scanning with the assistance of the plaintiffs, whose struggle it has always respected, in order that, when a site offensive is brought to its attention and on condition that it is manifestly intended essentially to French users, it might cease its hosting;

That to prove its good faith, it indicates that it has stopped the hosting of the protocol of the Sages of Sion, considering sufficient the link of attachment of such document with France due to the language of the work;

Whereas with a little goodwill, Yahoo! Inc. may convince itself of the utility of extending this link of attachment to photographs and to descriptions of objects representing symbols of Nazism;

Whereas according to the information in the experts' report upon request of the plaintiffs and which were not seriously contested, Yahoo! already refuses on its auction site the sale of human organs, drugs, works or objects related to pedophilia, cigarettes or live animals, all of which sales are directly excluded and for just cause from the protection of the first amendment of the American constitution which guarantees freedom of opinion and expression;

Whereas it would no doubt cost very little for it to extend these prohibitions to symbols of Nazism and such an initiative would have the merit of satisfying a requirements of ethics and morals which are shared by all democratic societies;

Whereas the combination of technical means available and of the initiatives which it can implement if only for the sake of elementary public morals therefore make it possible to satisfy the injunctions contained in the order of 22 May 2000 that is through filtering of access to the site auctioning Nazi objects as with the service involving the work *Mein Kampf* which was covered by the formulation of order cited above within the terms "and of any other site or service which contains an apology of Nazism";

Whereas a period of three months will nevertheless be allowed for compliance with this order;

Whereas beyond such period, it shall be liable to pay 100000 French francs per day of delay until execution shall have been fully accomplished;

With respect to the claim against Yahoo! France

Whereas the experts' report stipulates and suggests:

"Verify whether Yahoo! France has indeed complied with the terms of our injunction contained in the order of 22 May 2000."

The order of May 22, 2000 stipulated in this respect:

"[The Court] Orders Yahoo! France to warn any and all surfers consulting yahoo.fr, and the foregoing prior to use of the link enabling him to

pursue his search on yahoo.com where the result of his search, whether via the arborescence, or through the use of key words leads him to sites, pages or forums the title and/or contents of which constitute a violation of French law, as well for consultations of sites which display apologies of Nazism and/or exhibit uniforms, insignia, emblems reminiscent of those which were worn or exhibited by the Nazis, or offering for sale objects or works the sale of which is strictly forbidden in France, it must interrupt the consultation of the relevant site lest it incur the sanctions stipulated by French law or answer to actions initiated against it;"

To execute the terms of the order, Yahoo! France has:

- modified and completed the conditions of use which are accessible by clicking on the link "know everything about Yahoo!" which appears at the bottom of each of the pages on the site. The following paragraph has been added:

  "Also, if in the context of a search carried out on www.yahoo.fr from an arborescence, or using key words, the result were to lead you to point to sites, pages or forums the title and/or the contents of which constitute an infraction against French law, given in particular the fact that Yahoo! France cannot control the contents of such sites and external sources (including the contents referenced on other sites and services of Yahoo! throughout the world), you must interrupt your search of the site in question lest you incur the sanctions provided by French law or have to answer legal actions initiated against you."

- implemented, in the case of searches conducted by arborescence (categories) a warning thus formulated:

  "Warning: in pursuing your search your search on Yahoo! US you may be led to view revisionist sites the contents of which constitute an infraction against French law and the viewing of which, if you pursue it, will expose you to sanctions."

It has been observed that the conditions of use of Yahoo! were not systematically posted at the time of the first connection to such site and that moreover the link "know everything about Yahoo!" did not necessarily evoke the general conditions of use.

On the other hand, the warning was systematically posted in the context of searches by category (for example, *holocaust*).

It is technically possible for Yahoo! France to compel posting of its conditions of use at the time of the first connection by a user to its site.

Yahoo! might also, in addition to or in replacement of the preceding measure, provoke the systematic posting of the warning cited in 2) as soon as is posted the link to yahoo.com.

But, with respect to this last point, Yahoo! has pointed out that these were not the terms of the order. Accordingly, it will be up to the Court to interpret its decision. Contrary to what is maintained by Yahoo! "to warn internauts viewing Yahoo.fr, even before they use the link ..." may mean that the warning must be posted each time the link is posted.

Whereas Yahoo! France argues that it has fully complied with the terms of our order of May 22, 2000, in that it has modified the link subject of the plaintiffs' complaint, by installing the warning mentioned in the order on several links, and by reminding internauts of the conditions of use of the services which are accessible to users immediately upon their connection to yahoo.fr and which since 3 November 2000 may be viewed on all the pages of yahoo.fr, and by modifying the general conditions of use of the service by integrating a message which goes beyond even the prescriptions of the order of 22 May and this in the terms of the new article 6.2;

Whereas the initiatives of Yahoo! France are technically of a nature such as to satisfy for the most part the terms of our order of 22 May 2000, subject to the reservation however that the warning be mentioned each time the link is posted and "even before the internaut makes use of the link";

Now therefore

In public hearing in first instance, in the presence of the parties, we hereby:

- reject the objection to our competence presented by Yahoo! Inc.;
- order Yahoo! Inc. to comply within three months with the notice including an injunction of our order of 22 May 2000 lest it be liable to pay 100000 francs per day of delay commencing as of the first day following the expiration of a period of 3 months;
- designate Mr Wallon, 19 rue Decamps, 75016 Paris, telephone: 0147554773, Fax: 0147554808 for the purpose of rendering an advisory report with respect to the implementation of the terms of the above order;
- set at an amount of 10000 francs the provision for the cost of the consultant's report which shall be paid by Yahoo! Inc. directly into the hands of the consultant within one month of this order;
- declare that should the provision not be paid in a timely manner, the matter shall be referred to us;
- recognise that Yahoo! Inc. has decided to stop hosting of the protocol of the Sages of Sion;
- note that Yahoo! France has for the most part fulfilled the letter and the spirit of the decision of 22 May 2000 which contains an injunction applicable to Yahoo! France;
- order however that it cause to appear a warning to the attention of internauts even before they use the link to yahoo.com and the foregoing within two months of the date of this decision;
- order Yahoo! Inc. to pay to each of the plaintiffs an amount of 10000 francs under the terms of Article 700 of the New Code of Civil Procedure;
- declare that it is not appropriate to apply the above measures to Yahoo! France;

We reserve for ourselves the eventual liquidation of the injunction;

We declare that that it is not appropriate to order any other measures nor to consider the other claims against Yahoo! France;

We order that Yahoo! Inc. shall bear the costs of the case, except for those arising in connection with claims made against Yahoo! France which shall provisionally remain for the account of each of the parties.

Done in Paris on 20 November 2000

The Clerk of the Court
Nicole VOURIOT

The Chief Justice
Jean-Jacques GOMEZ

Appendix 6. Catalogue of vital and significant traffic data[1]

General overview of data at the different levels

Although administrative information is not part of the traffic data, there has to be a link between traffic data to this administrative information so that identification of the subscriber is possible. Therefore we give here also the overview of these data.

1.1. Subscriber/Administrative information on the different levels

- name and first name
- address
- telephone number (fixed and/or mobile), other contact information (e-mail, aliases, ...)
- subscriber identification (e.g. IMSI, MSISDN,)
- equipment identification (e.g. IMEI, Serial modem number, MAC)
- date and time of the creation of the account
- subscriber's IP address while creating the account
- subscriber's user identification (login name)
- subscriber's user password
- subscriber's bank account information if he pays for this subscription

1.2. Level 1: the data/signal carrier level

- called number (even if the call was unsuccessful)
- calling number (even if the call was unsuccessful)
- intermediate numbers in case of call forwarding or conference calls
- date and time of beginning and end of the communication or start plus duration
- type of communication (e.g. incoming/outgoing/conference/forwarded/bearer services, etc.)
- geographical location where the end-user devices connect to the telecom network
- identification numbers of the end-user device connecting to the telecom network

1.3. Level 2: the data network level

- level 1 protocol subscriber identification (e.g. IMSI, MSISDN, serial modem number, etc.)
- network user address (e.g. for the Internet: the end-user IP address – static or dynamic)
- date and time of beginning and end of the network connection or start plus duration
- data volume in/out

1.4. Level 3: telecom application level

- level 2 protocol identifier of the sender (e.g. IP address of the sender)
- level 3 protocol identifier of the sender (e.g. e-mail address of the sender or nick for IRC)
- level 3 protocol identifier of the destination
- date and time of use of the level 3 telecom application or service
- message identifier

Detailed overview

1.5. At level 1: the data/signal carrier level

1.5.1. Fixed line telephony

1.5.1.1. Vital

- calling number ID
- called number (receiver)
- time/date start connection
- time/date end connection
- carrier service (tele- and/or bearer service)

1.5.1.2. Significant

- unsuccessful calls information (reason why)
- intermediate and rerouting numbers in case of call forwarding and conference calls

1. Updated on 27 November 2001.

The log must show telephone numbers for calling and called parties.

For incoming calls, the 'A' number must be provided, even for numbers that have blocked caller ID detection and for overseas telephone numbers.

1.5.2. Mobile phone (GSM, Satellite, UMTS, etc.)

1.5.2.1. Vital in addition to the fixed systems requirements

- subscriber identification (e.g. IMSI number)
- equipment identification (e.g. IMEI number)
- location information (e.g. cell where the device connected to the network)

1.6. At level 2: data network level

1.6.1. Internet access

1.6.1.1. Vital

- link to level 1
- equipment identification (e.g. serial modem number, MAC, etc)
- caller line identification (if available)
- subscriber identification
- IP address used by the end-user – static or dynamic
- date and time of beginning and end of the network connection or start plus duration

1.6.2.1. Significant

- data volume in/out
- IP address of intermediate server (e.g. proxy server)
- IP address of requested destination server/computer
- called telephone number of destination server/computer if applicable (e.g. POP address)

The log of the use of IP addresses must show clearly which user accounts were used for the connection, in such a way that the name and address of the user can be produced.

The log must also show from which telephone number the connection call was made or the physical address of the system that was used. This applies also in cases where several different companies are used.

1.7. At level 3: telecommunication application or service level (e-mail, ICQ, SMS, etc.)

The services offered at this level are numerous and very different one from another.

Although there is no agreement if and for which of these services traffic data should be considered as vital, the members of the EWPITC see a need to qualify following services **as significant** and ask thus for those to retain the traffic data:

- e-mail
- SMS gateways
- Website publishing (Website or announcements on websites)
- newsgroups

1.7.1. Proxy servers

If Internet users perform their Web activities through a proxy or cache server, the only IP address that the visited Website can register is that of the proxy server. The Website cannot differentiate any of the users coming via the same proxy server.

The providers of this proxy service have to be able to link the used web service further on to the real end user.

- IP end user
- IP proxy server
- IP requested server
- date and time of the request

1.7.2. E-mail

- e-mail address sender
- e-mail address receiver(s) (also "CC" and "BCC")
- message ID
- mail size
- type of service/communication protocol (SMTP)
- IP address of the sender

1.7.3. SMS gateway

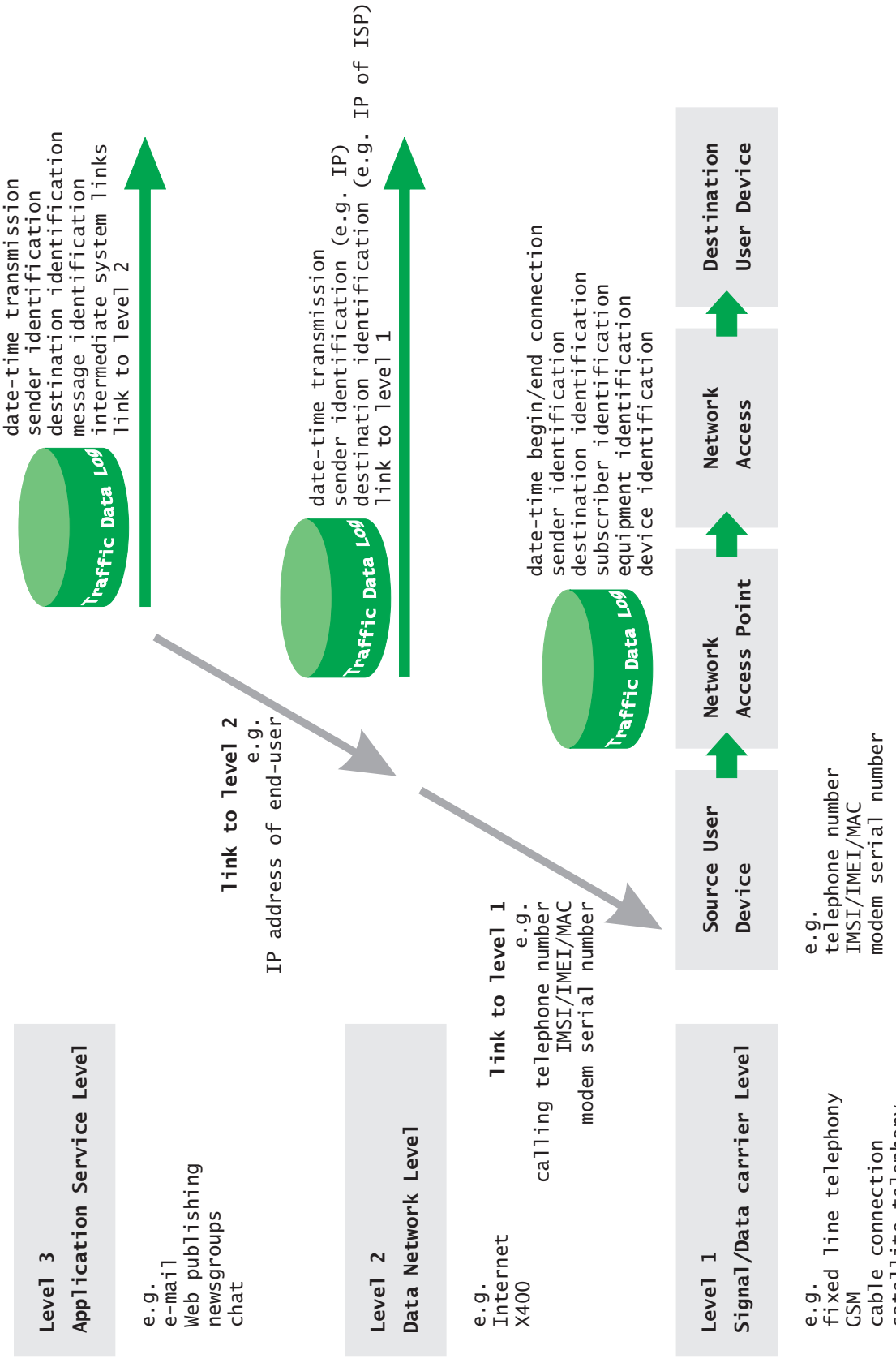
- IP address of the user filling in the SMS message
- date and time of when the message was received on the Website of the gateway
- called GSM number
- GSM number of the SMS gateway
- date and time of passing the message to the GSM SMS service

1.7.4. Website publishing

- IP address of the user uploading the website
- account identification of the publishing user
- date and time of when the website upload was done.

Appendix 7. Schematic representation of the layered approach to determine data traffic to retain

EWPITC Interpol



Appendix 8. Chapter V of Recommendation No. R (2000) 11 of the Committee of Ministers to member states on action against trafficking in human beings for the purpose of sexual exploitation

V. Assistance to and protection of victims

i. Victim support

26. Encourage the establishment or development of reception centres or other facilities where the victims of human trafficking can benefit from information on their rights, as well as psychological, medical, social and administrative support with a view to their reintegration into their country of origin or the host country.

27. In particular, ensure that the victims have the opportunity, for example through the reception centres or other facilities, to benefit from legal assistance in their own language.

ii. Legal action

28. Provide, where possible, victims of trafficking, particularly children and witnesses, with special (audio or video) facilities to report and file complaints, and which are designed to protect their private lives and their dignity and reduce the number of official procedures and their traumatising effects.
29. If necessary, and particularly in the case of criminal networks, take steps to protect victims, witnesses and their families to avoid acts of intimidation and reprisals.
30. Establish victim protection systems which offer effective means to combat intimidation as well as real threats to the physical security of the victims and their families both in countries of destination and countries of origin.
31. Provide protection when needed in the country of origin for the families of victims of trafficking when the latter bring legal proceedings in the country of destination.

32. Extend, where appropriate, this protection to members of associations or organisations assisting the victims during civil and penal proceedings.

33. Enable the relevant courts to order offenders to pay compensation to victims.

34. Grant victims, if necessary, and in accordance with national legislation, a temporary residence status in the country of destination, in order to enable them to act as witnesses during judicial proceedings against offenders; during this time, it is essential to ensure that victims have access to social and medical assistance.

35. Consider providing, if necessary, a temporary residence status on humanitarian grounds.

iii. Social measures for victims of trafficking in countries of origin

36. Encourage and support the establishment of a network of NGOs involved in assistance to victims of trafficking.

37. Promote co-operation between reception facilities and NGOs in countries of origin to assist the return and reintegration of victims.

iv. Right of return and rehabilitation

38. Grant victims the right to return to their countries of origin, by taking all necessary steps, including through co-operation agreements between the countries of origin and countries of destination of the victims.
39. Establish, through bilateral agreements, a system of financing the return of victims and a contribution towards their reintegration.
40. Organise a system of social support for returnees to ensure that victims are assisted by the medical and social services and/or by their families.
41. Introduce special measures concerned with victims' occupational reintegration.