



Protecting Children Online

An ECPAT Guide



Protecting Children Online: An ECPAT Guide

Editor and Researcher: Carol Livingston

**With thanks to Riitta Koskela for original text,
and John Carr, Muireann O Briain, Mark Hecht, Denise Ritchie
and Agnes Fournier de St. Maur for technical advice and
contributions to the text.**

**Illustrations by Katarina Dragoslavic
2nd Edition updated and edited by Sarah Kay**

**© Copyright: ECPAT International, 2000
1st Edition: July 2000
2nd Edition: May 2002**

**328 Phayathai Road, Ratchathewi, Bangkok 10400
Tel: 662-215-3388, 611-0972
Fax: 662-215-8272
Email: info@ecpat.net
Website: <http://www.ecpat.net>**



**A portion of the printing costs of the 2nd edition was provided by the
Foreign and Commonwealth Office of the United Kingdom**



TABLE of CONTENTS

• Introduction	2
Internet	4
• What are the new technologies and how do they work?	4
• What is an ISP and why are ISPs important?	5
• How do people communicate?	8
Dangers	13
• What other common software do child exploiters use?	13
• Why do child exploiters like new technology?	15
Legal issues	18
• What is child pornography?	18
• Why is child pornography a key issue?	19
• What steps have been taken internationally?	20
• What are the major legal issues?	22
• What about freedom of expression?	26
Protecting Children	29
• What can protect children on the Internet?	29
• How do filtering and rating software packages work?	31
• What is being done now?	34
• What can you do?	38
Additional Reading	44
• Online Links	45
• Hotlines	49
Appendices	51
I ECPAT Policy on Child Pornography	51
II Lexicon	53





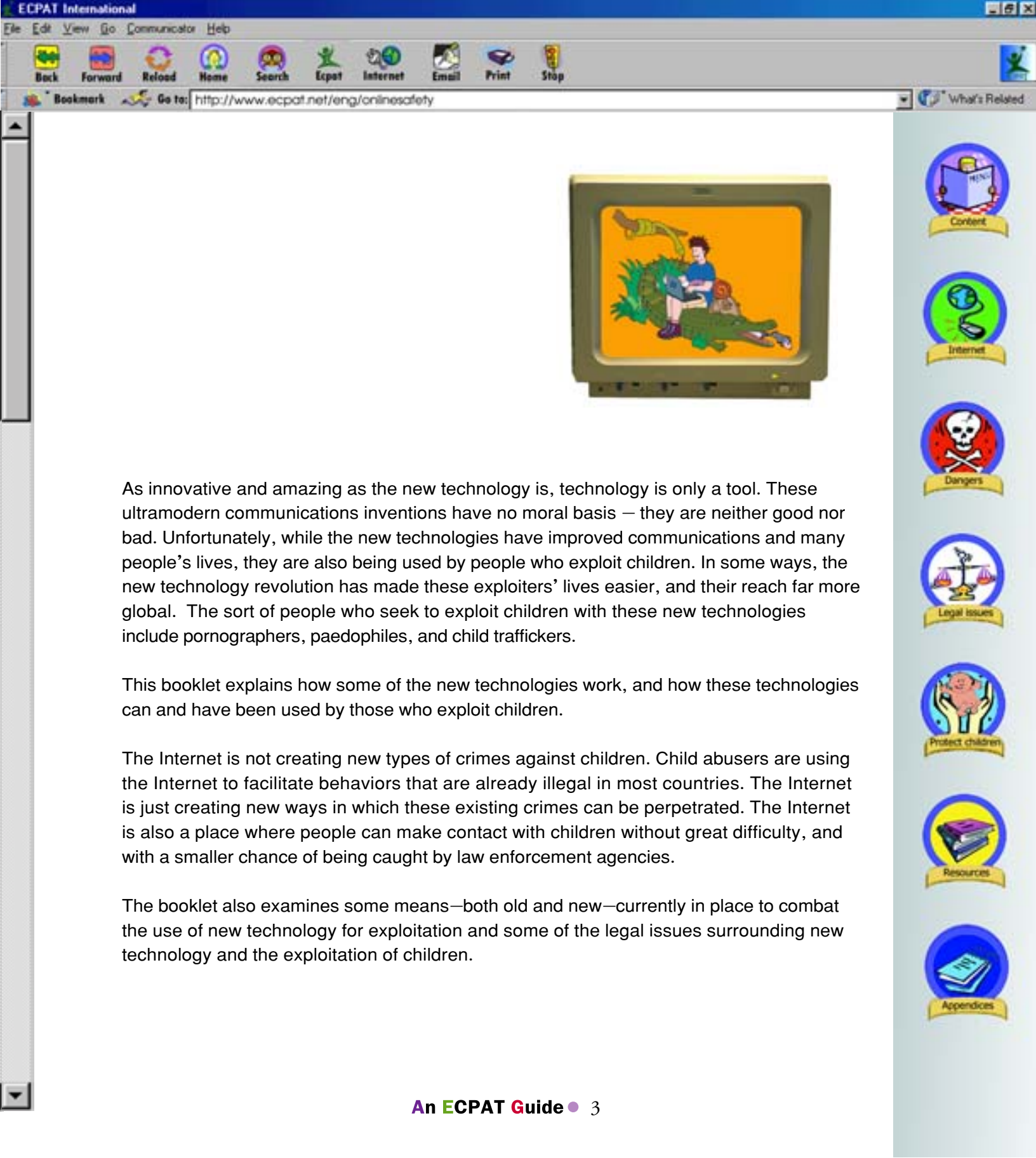
Introduction

The speed at which new technology is changing our ability to communicate, and creating new ways to communicate, is staggering.

Five years ago, it was hard to imagine that tourists would be able to send e-mail from the ancient capital of Luang Prabang, buried in the jungles of Laos, that nearly 50% of Australians and 57% of South Koreans would have internet access,¹ or that a grandmother in Moscow with a tiny camera attached to her computer could be able to see and talk with her grandchildren in Sao Paolo at no more cost than that of two tiny cameras and the internet connection.

For less than US\$600 anyone in the year 2002 can have the computing and communications power that only a few years ago cost major corporations hundreds of thousands of dollars. Now anyone with an email account and a scanner can send photos to their friends and families. They can merge two photos into one or “morph” the images, changing the picture completely to create a new reality. Instant chat allows people to make new friends around the world, or to keep up with old ones. With widely available video conferencing packages, real-time meetings and real time live “shows” can be held with participants from around the world.

¹ Nielsen Net Ratings



As innovative and amazing as the new technology is, technology is only a tool. These ultramodern communications inventions have no moral basis – they are neither good nor bad. Unfortunately, while the new technologies have improved communications and many people’s lives, they are also being used by people who exploit children. In some ways, the new technology revolution has made these exploiters’ lives easier, and their reach far more global. The sort of people who seek to exploit children with these new technologies include pornographers, paedophiles, and child traffickers.

This booklet explains how some of the new technologies work, and how these technologies can and have been used by those who exploit children.

The Internet is not creating new types of crimes against children. Child abusers are using the Internet to facilitate behaviors that are already illegal in most countries. The Internet is just creating new ways in which these existing crimes can be perpetrated. The Internet is also a place where people can make contact with children without great difficulty, and with a smaller chance of being caught by law enforcement agencies.

The booklet also examines some means—both old and new—currently in place to combat the use of new technology for exploitation and some of the legal issues surrounding new technology and the exploitation of children.



Internet

WHAT ARE THE NEW TECHNOLOGIES AND HOW DO THEY WORK?

The Internet

The Internet is a worldwide network of computers. The theory behind the Internet is simple: any link in the system can help send data to its destination, even if the sending and receiving computers are not directly connected. The Internet can be used to send e-mail messages and computer files between any number of people. The Internet is also home to the World Wide Web, a vast series of “web sites” which contain information and which may be linked to other sites.

Information sent over the Internet does not take a predefined route. The Internet tries to avoid “traffic jams.” It finds the most efficient quickest way to get information to the intended recipient even if that means routing data via computers in other countries. A file sent from London to Birmingham could go via computers in San Francisco, Atlanta, and Lagos if that route was quickest.

Today the Internet has around two hundred million users worldwide who can communicate with each other.





WHAT IS AN ISP? WHY ARE ISPs IMPORTANT?

Internet Service Providers (ISPs) are the backbone of the Internet. ISPs run the computers which make up the Internet. These computers are usually referred to as “servers.” They are the point of entry to the Internet for most individual users.



ISPs provide dial-up access to the Internet, where users gain access to newsgroups, e-mail, and chat. Users can also upload and download files in various ways on the Internet, and ISPs provide the mechanisms for this exchange of files. For anyone who wants to run their own web site, ISPs provide storage and an address on the Internet to which computers look for information whenever anyone wants to access that site.

ISPs often also offer “mirroring” services to web site owners. Mirrored sites are often far away from the physical location of the main web site. Popular file download sites may have a main server in the United States, but they may also have their site mirrored on European or Asian servers to speed up access on those continents. These mirroring ISPs simply provide quicker access to the same information as held on the main site.

ISPs assign IP (internet protocol) addresses to individual computers which use their service to log onto the Internet. The IP address is a number that identifies a particular computer on the Internet and tells the other computers where to find it.

While some IP addresses are assigned specifically to one computer, ISPs often use a “dynamic” IP address system. Dynamic IP addresses are not attached to one computer. Any number of users might use the same dynamic IP address within the same day.





Each ISP has a certain set number of addresses to assign users as they try to log onto the Internet. A dynamic system randomly allocates an address each time a user logs on. If a user logs on at 5:01 pm and is given a dynamic IP address, then logs off and logs back on at 5:02 pm, the user will most likely be given another IP address number for the second session.



Dynamic IP addresses are a useful way of allocating Internet resources and controlling Internet traffic. However, the only way dynamic IP addresses can be traced to individual users is by checking the ISP's usage log to see what user account was assigned that IP address at a specific time. Logs can also reveal from what telephone number the call to connect to the IP was made.



ISPs keep logs of dynamically assigned IP addresses and subscriber information that can provide crucial links for finding child exploiters who use the Internet. While most ISP subscriptions are paid for by credit card or a bill sent to a home address, sometimes user accounts are set up on a pre-pay system. Other times the subscriber may pay by postal order, or use a post office box as an address. Logs which trace a specific calling line number to a specific IP address and time are thus very important in prosecuting crimes which utilize the Internet against children.



In a number of countries so-called "free" ISPs have now emerged. There is no charge for the Internet connection that these ISPs provide except for the cost of the call. Once an individual has joined a free ISP service there are usually few attempts to verify the true identity of a user. This can allow easy access to bogus, cost-free Internet identities. Law enforcement officials need the full co-operation of ISPs in order to be able to apprehend offenders who may use the Internet under one of these aliases.



ISPs may fear that they will infringe civil liabilities if they release personal information about subscribers without warrants. Also, legislation requiring ISPs to retain or release such data may conflict with other privacy or telecommunications legislation.



Some countries have introduced legislation that puts a positive obligation on ISPs to monitor content on their servers and prescribe penalties for those who do not comply.



CASE EXAMPLE - BUFFNET

In 1998, the New York State Attorney General's Office and the State Police began an investigation of a group that called itself "Pedo University", whose members used the newsgroup to possess and exchange child pornography. After a series of successful prosecutions that helped to dismantle "Pedo U" the investigation turned its focus from the users of the newsgroup to the ISPs that provided access to the newsgroup. One of these was Buffnet. When Buffnet was made aware of the content of the newsgroup, it took no action.

In February 2001 Buffnet, a large regional ISP based in West Seneca, New York outside of Buffalo, pleaded guilty to the crime of Criminal Facilitation in the Fourth Degree, a Class A misdemeanor. The company admitted that it failed to take action when it was notified by a customer as well as by law enforcement that one of the newsgroups it carried was being used to distribute graphic child pornography. Buffnet was fined US\$5000, however the cost of the bad publicity the prosecution created is immeasurable.

"When BuffNet, or any ISP, is informed of this kind of heinous criminal activity, it has a duty to act. Here, Buffnet chose to look the other way," New York Attorney General Eliot Spitzer said. "This response is not defensible by any standard of law or conscience."

Until now, prosecutions in this area focused primarily on individuals who subscribed to an ISP like BuffNet, and who logged on to a newsgroup and downloaded and traded in child pornography. In this case the Attorney General's investigation widened its focus to include the ISP that knowingly provided the means and the opportunity for this criminal conduct to occur¹.



¹ Office of the New York State Attorney General - Press Release dated February 16 2001



HOW DO PEOPLE COMMUNICATE?

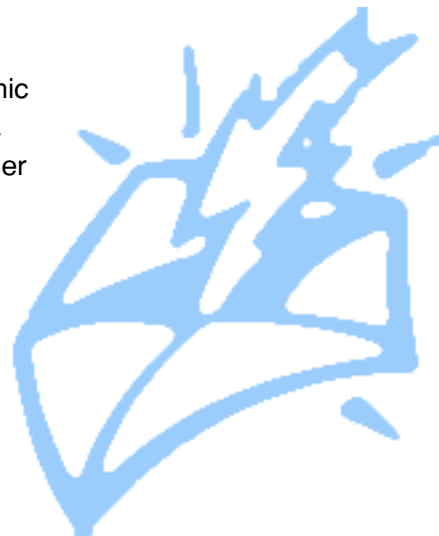
E-mail

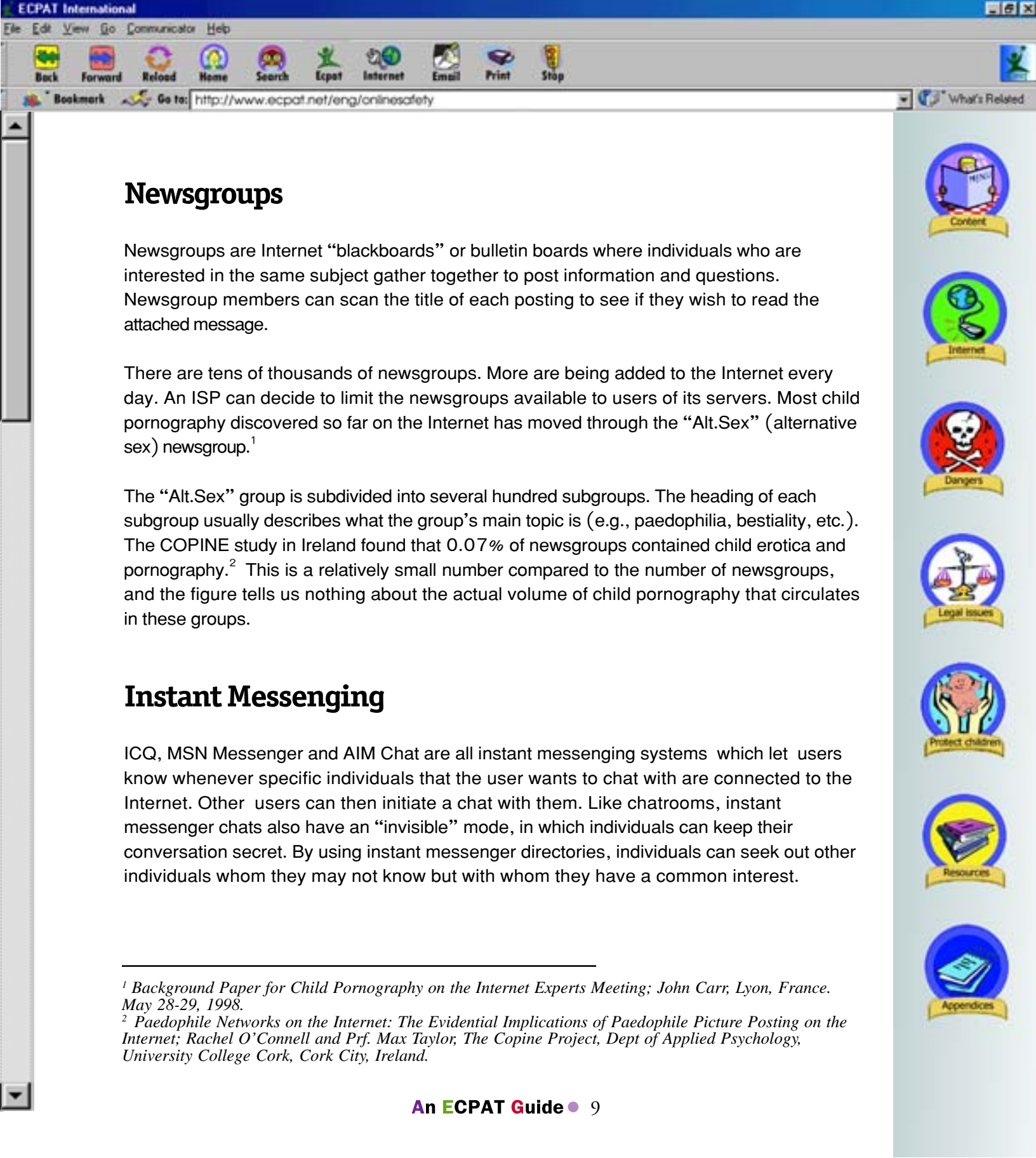
As most people know, e-mail usually means electronic letters that are sent between users on the Internet. E-mail can be simple text messages or can have other files attached. They can also contain graphic, audio and/or video information.

E-mail accounts are usually free when a customer buys Internet access from an ISP. If the ISP has verified who the account-holder is through such means as requiring credit card details, the ISP knows who is responsible for the email coming from that e-mail address.

Headers in e-mail messages tell the recipient who sent a message and the path that message traveled. With many text e-mail systems, the e-mail software automatically inserts the IP address from which the message originated and the time it was sent in the e-mail's header. The header of the message often includes a list of computers on the Internet through which the message traveled to get from sender to recipient.

Free Internet e-mail accounts are universally available through the World Wide Web from such sites as Yahoo! or Hotmail. E-mail to and from these addresses is retrieved only via websites. As with free ISP services, it is easy for users to create fake identities on many free e-mail systems. When a user signs up for a free e-mail account usually there are no security checks to verify whether information such as the user's name and address entered on the e-mail application is correct.





Newsgroups

Newsgroups are Internet “blackboards” or bulletin boards where individuals who are interested in the same subject gather together to post information and questions. Newsgroup members can scan the title of each posting to see if they wish to read the attached message.

There are tens of thousands of newsgroups. More are being added to the Internet every day. An ISP can decide to limit the newsgroups available to users of its servers. Most child pornography discovered so far on the Internet has moved through the “Alt.Sex” (alternative sex) newsgroup.¹

The “Alt.Sex” group is subdivided into several hundred subgroups. The heading of each subgroup usually describes what the group’s main topic is (e.g., paedophilia, bestiality, etc.). The COPINE study in Ireland found that 0.07% of newsgroups contained child erotica and pornography.² This is a relatively small number compared to the number of newsgroups, and the figure tells us nothing about the actual volume of child pornography that circulates in these groups.

Instant Messaging

ICQ, MSN Messenger and AIM Chat are all instant messaging systems which let users know whenever specific individuals that the user wants to chat with are connected to the Internet. Other users can then initiate a chat with them. Like chatrooms, instant messenger chats also have an “invisible” mode, in which individuals can keep their conversation secret. By using instant messenger directories, individuals can seek out other individuals whom they may not know but with whom they have a common interest.

¹ *Background Paper for Child Pornography on the Internet Experts Meeting; John Carr, Lyon, France. May 28-29, 1998.*

² *Paedophile Networks on the Internet: The Evidential Implications of Paedophile Picture Posting on the Internet; Rachel O’Connell and Prf. Max Taylor, The Copine Project, Dept of Applied Psychology, University College Cork, Cork City, Ireland.*





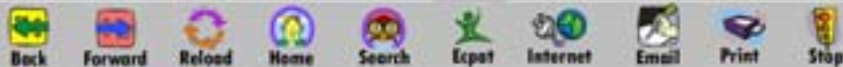
Chat Rooms

Chat Rooms allow two or more people to “speak” over the Internet using text messages. Chat Rooms are particularly popular with children and teens. Individuals often use pseudonyms in chat rooms.

Chat Rooms are divided by channels. The channels are usually named to give an indication of what the conversation in the channel should be about. Users can also hold private conversations within most channels, agreeing to leave the chat room so that they can talk to each other without anyone else being able to see what the conversation is about.

While some chat rooms are monitored for inappropriate language and content, others are not. Child abusers will sometimes enter chat rooms and pretend to be children in order to elicit information from real children and to gain their confidence, often with the intention of trying to meet a child in real life in order to abuse them. The abuser may also try to persuade the child to take pornographic pictures of themselves or their friends to send over the Internet.





Video Conferencing And Telephony



Real time video conferencing software is probably even more widely available than Internet telephony software. Microsoft's free NetMeeting software is usually installed with Microsoft's most recent operating systems. With a small digital camera, available in most countries for under US\$ 100, groups can have real time meetings with video and sound.

Instant messaging software is able to be used with various different video conferencing software packages like **NetMeeting**. Microsoft also provides a directory of NetMeeting users, which allows NetMeeting users to seek out others.

As with much new Internet technology, there has reportedly been a great deal of sexual activity on the net using video conferencing technology.¹

While the great majority of this activity has been between adults, what may have been the first case of real-time video transmission on-line of children being sexually molested occurred in 1996.

The Orchid Club

The Orchid Club international child pornography ring was broken in 1996 by the San Jose, California police. The Orchid Club was discovered when the police arrested one of the members on a charge of child sexual abuse. Involving individuals from countries as far afield as Finland, Australia, the United Kingdom and Canada, the Orchid Club is widely considered the first prosecuted case in which pictures of a child being molested were transmitted in real time using video conferencing software. Via the Internet at least 11 men who belonged to the club watched the molestation of a young girl and participated by sending requests to the man abusing her, asking for various poses and abuse.

¹ [Http://www.salon.com](http://www.salon.com)





Bulletin Boards

Bulletin boards were one of the earliest mechanisms for exchanging information between remote computers. One computer dials directly into another computer which acts as a “host” for the bulletin board.

Bulletin boards are normally private servers from which files can be downloaded or where messages can be posted for other users of the bulletin board. IP addresses are neither used nor needed because the connection is direct.

Bulletin boards are not strictly part of the Internet, where they have been largely superseded by newsgroups, which might also be referred to as “bulletin boards.” Old-fashioned bulletin boards are still used, often by groups that wish to avoid detection.



Dangers

WHAT OTHER COMMON SOFTWARE DO CHILD EXPLOITERS USE?

Encryption software

Encryption software locks a file or message. Only users with the same encryption software, or the necessary password to open the file, can read files which have been encrypted. So-called “keys,” which are sometimes based on randomly generated numbers, are usually used to open the files. There are many different encryption packages commonly available. Encryption software is embedded in many computer programs, from electronic garage door openers to ATM machines.

Attempts have been made in several countries to make “key escrow” of encryption software mandatory. Under the various key escrow plans, either the makers or the users of encryption software would lodge with governments or designated “third parties” the keys to the software that would allow law officials to read any file.

While supporters of key escrow feel that access to encryption keys is critical in order for law enforcement to be able to do their job properly, many opponents to key escrow fear misuse of the escrow system. Critics of the plan point out the potential for human error or abuse of the system and the technical problems inherent in the plan.¹ China has recently demanded that “keys” to encryption software be lodged with that government.

¹ See, *The Risk of Key Recovery, Key Escrow, & Trusted Third Party Encryption, A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, Hal Abelson and Whitfield Diffie, et al.,* <http://www.cdt.org/crypto/risks98>





Graphics and Morphing Software

Digital technology has helped make pornography a cottage industry. With a cheap scanner, anyone can put their pictures on the web, or email them to others.

Digital graphics software (Photoshop, Illustrator, Microsoft PhotoEditor, etc.) can be used to change pictures. After a picture has been scanned into the computer, these image editing programs can be used to put several photos together or to distort pictures and create a believable image of a reality that never existed. The distortion and change is called “morphing.”

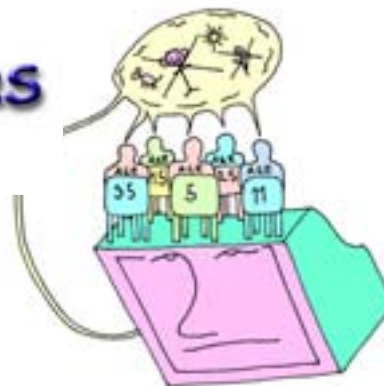


Because many child exploitation and pornography laws deal only with real children and depictions of events which actually occurred, defendants may claim in court that a morphed picture, no matter how disturbing, is not a picture of a real child or a situation which actually took place, and may thus not be illegal. However, in some countries, such as the United Kingdom, even artificial or morphed pictures of child pornography are illegal and are treated in law exactly as if they were real.



WHY DO CHILD EXPLOITERS LIKE NEW TECHNOLOGY?

Child exploiters like new technology for the same reasons everyone else does: new technologies have made it easier, faster and cheaper to communicate, especially with people who are far away.



“Before computers, distributors of child pornography used the mail or underground distribution networks. Consumers and distributors had to actually know one another to trade or exchange material. With the Internet, the pornography becomes readily accessible to anyone – it appears instantly.”¹

Child exploiters use the Internet to validate their beliefs. By finding others on the net who agree with their values, they reinforce, rationalize and legitimize their belief that they are doing nothing wrong. They encourage others to join their activities, and will seek others out in chat rooms to trade information and to bring into the “network.”

By using the Internet, people who look for child pornography can have instant gratification. They can download new photos immediately rather than waiting for them to arrive in the mail. Those who want to meet children will troll the online chat rooms, often pretending to be children themselves in order to gain real children’s confidence.

The Internet has also made it easier for child abusers to extend that global reach. In one case, 50,000 images of child pornography were found on a server based in Moscow but directed by email from the United States. The owner charged US\$ 100 a month to download his password-protected images.

Child sex tourism is now being marketed globally on the Internet by spreading information about the potential for sexual abuse in countries where poverty may make abuse easier. In 2001, a research project was undertaken by ECPAT and Casa Alianza, a non-profit organisation working for street children in Central America. The research

¹ *Innocence Exploited: Child Pornography in the Electronic Age.* Skoog, Douglas and Jane Murray, Canadian Police College, University of Winnipeg, 1998.





showed that the Internet had as many as 40 pages directly promoting Costa Rica alone as a “sex tourism destination”. These pages contained explicit testimonials from tourists highlighting the best hotels, pick up points and the “going rate” for commercial sex.



Even more disturbing, was the research conducted on www.latinchat.com. On this site the researchers found they could get free access to an enormous assortment of child pornography. They also found that when they posed as a 13 year old Mexican boy who entered a chatroom they received an incredible 102 e-mails over four hours directly seeking sexual information and proposing personal meetings.



The research team also investigated the “boy love” group which goes by the acronym “FPC” this group has it’s own website which links child sex abusers around the world. They found that by simply subscribing to one of the websites’ lists, they received hundreds of e-mail messages attaching texts and graphics with sexually explicit depictions of young boys. One of the members of this “boy love” association was an employee of the University of Costa Rica, who with unlimited access to the Internet through the University introduced young children of limited resources and filmed them while having sexual relations with them. He “freezes” these images and then sends the photos through the Internet via groups like FPC.



Like all criminals, those who exploit children like the anonymity of the Internet. By using pseudonyms in chat rooms, fake e-mail addresses, and software which strips out any information from an e-mail which might be used to trace them, they hope to cover their tracks and avoid prosecution. They also take advantage of the international nature of the Internet, setting up websites and storing files on servers which are located in countries or jurisdictions with lax child pornography or child protection laws.



Wonderland was the first highly publicised international operation that successfully prosecuted child sex abusers around the world. In an operation co-ordinated by Interpol, on September 1, 1998 more than 100 people allegedly involved in the Wonderland Club were arrested in 12 countries and more than 1 million pornographic images with children as young as 2 were found.¹



Since Wonderland, law enforcement agencies around the world have been working together to seek out and prosecute child sex abusers on-line.

¹ *The Sexual Abuse of Children via the Internet: a new challenger for Interpol* Agnes Fournier de Saint Maur, *International Conference Combating Child Pornography on the Internet*, Vienna, 29 September-1 October, 1999.



Law Enforcement Operations that Catch Child Sex Abusers On-Line

August 2001:- Operation Avalanche

Landslide Productions was incorporated in Dallas by its directors Thomas and Janice Reedy in 1997. Initially, the company offered explicit material involving mostly adults but as the business grew, the Reedys derived more and more of their income from providing access to Web sites featuring child pornography. Landslide had a fee-sharing arrangement with foreign Web masters who maintained the child pornography, the Reedys grossed about \$US5.7 million from subscribers and paid about 60 percent to foreign Web masters in countries including Russia and Indonesia. The company was very profitable, taking in as much as \$US1.4 million in one especially lucrative month. It is the largest known commercial child pornography enterprise uncovered. Its Web site counted at least 250,000 subscribers, many of them living overseas. US investigators and international law enforcement bodies began investigating Landslide in 1999 after receiving more than 250 complaints from computer users around the world. Thomas and Janice Reedy were arrested in September 1999 and law enforcement seized control of the company and turned their attention to consumers. Pretending the company was still active, investigators sent electronic messages to subscribers to determine who would buy the illegal materials. In August 2001, US and other US law enforcement bodies set up a sting operation that would catch subscribers "picking up" their illegal material. In the US alone over a 100 people were arrested.

November 2001:-Operation Landmark

"Operation Landmark" focused on child sex abusers who downloaded and distributed child pornography from the Internet. Police in 19 Countries executed 130 searches and arrest warrants, acting on information supplied by Interpol.

Police monitored traffic, an Internet service provider "Demon Internet", who agreed to co-operate with them and allow access to its servers. One of the identified news groups was used by abusers to seek advice on how to "groom" young children for abuse. The investigators discovered that a little over 11,000 Internet users were downloading and distributing child pornography through 30 sites. However, they narrowed their investigation to the 400 distributors of the child pornography. Sadly, the investigators reported that these on-line sex abusers have learnt lessons from the Wonderland and Avalanche Operations and have been developing new and innovative ways to hide their true identities.





Legal Issues



WHAT IS CHILD PORNOGRAPHY?

Understanding what is child pornography is one of the most difficult aspects of dealing with the problem. There are many cultural interpretations of what is obscene or suggestive. In some cultures, “erotica” would be considered pornographic.



Many people find it difficult to imagine pornographic images of children, and therefore do not understand what is meant by ‘child pornography’. Also among the issues which cause disagreement are the age of consent to sexual relations, whether simple possession of child pornography should be a crime, whether an actual child had to be involved and whether morphed images constitute pornography.



Interpol’s Specialist Group on Crimes against Children states that “child pornography is the consequence of the exploitation or sexual abuse perpetrated against a child. It can be defined as any means of depicting or promoting sexual abuse of a child, including print and/or audio, centered on (a) sexual act or the genital organs of children.”



The Optional Protocol to the Convention on the Rights of the Child on Sale of Children, Child Prostitution and Child Pornography defines child pornography as ‘any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristic of which is depiction for a sexual purpose.’



Child pornography can exist in different forms. Visual child pornography is the most common, meaning the visual depiction of a child engaged in explicit sexual activity, real or simulated, or the lewd exhibition of genitals. Audio child pornography is the use of any audio devices using a child’s voice, real or simulated, intended for the sexual gratification of the user. Child pornography can also be simple text that describes sexual acts or is intended to provide sexual gratification.





WHY IS CHILD PORNOGRAPHY A KEY ISSUE?

Pornographic photos and videos are usually irrefutable evidence that child abuse has occurred. Pornography involving children is exploitation and the abuse of power over the object of the pornography, and even over children who have been obliged or seduced into watching it. It is often related to the trafficking of children, because children are trafficked from one country to another to be used for the making of child pornography.

There are vast amounts of child pornographic images available on the Internet. This is because the Internet has made it possible to multiply images without limit, and to transfer them with ease. The Internet has turned the collection of child pornography into a huge cottage industry.

Photos of child abuse sometimes come in numbered series to facilitate identification and collection. The collectors try to fill in series of photos. In some recent photos, the real name of the child was given. Photos can also be part of a narrative, with each new photo moving the story along.

Child pornography helps abusers rationalize their desire for children. Often the children are made to look smiling and compliant, as if they are enjoying the experience.

For the child involved, there are long-term consequences of child pornography. Whether or not the individual who created the pornography is prosecuted, once a pornographic picture is in the public domain it is likely to continue to be distributed and may haunt that child forever.

Child pornography also may be used as a tool to lower a child's inhibitions and, by showing other children in pornographic poses, entice that child into compromising situations.

The link between mere possession of child pornography and abuse of children is strong. It has been suggested that a large number of individuals who possess child pornography also sexually abuse children.





WHAT STEPS HAVE BEEN TAKEN INTERNATIONALLY?



The Convention on the Rights of the Child provides the basis for the work of international, national and local non-governmental organisations and law enforcement agencies in protecting children from Internet-related abuse. Governments which have ratified the Convention have an obligation to create a legal system in which children's rights—including the right not to be abused—are respected. The Convention on the Rights of the Child came into force on September 2, 1990, and at the time of publication, 191 countries had ratified it. (Every country in the world except for Somalia and the United States of America.)



Child pornography in any form is an abuse of the rights of children

This is clearly stated in the UN Convention of the Rights of the Child which most governments in the world have agreed to uphold.



*The Convention on the Rights of the Child, in Article 34 states that:
 “States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:



- a) The inducement or coercion of a child to engage in any unlawful sexual activity
- b) The exploitative use of children in prostitution or other unlawful sexual practices
- c) The exploitative use of children in pornographic performances and materials”



In the last decade, governments around the world have been made aware of the need for concerted action. As a result, the first World Congress against Commercial Sexual Exploitation of Children was held in Stockholm in August, 1996.

An Agenda for Action was adopted unanimously by 122 governments represented at the Congress. The Agenda asked governments in cooperation with NGOs, INGOs, and relevant members of the civil society to work together to face the growing challenge of child prostitution, child pornography and the trafficking of children for sexual purposes.

More recently, 159 governments, NGOs and INGOs have affirmed their commitment to work together to combat these challenges at the Second World Congress held in December 2001 in Yokohama, Japan.

The Optional Protocol to the Convention on the Rights of the Child

On 25th May 2000 an Optional Protocol to the Convention on the Rights of the Child was adopted by the General Assembly of the United Nations on the subject of sale of children, child prostitution and child pornography. The Optional Protocol entered into force on 18 January 2002.

The Protocol extends some of the measures contained in the Convention on the Rights of the Child. It takes into account particular concerns, including concerns about child pornography expressed in Vienna 1999 at the International Conference on Combating Child Pornography on the Internet.

Under the provisions of the Protocol, states who ratify it must ensure that production, distribution, dissemination, importation, exporting, offering, selling or possessing child pornography are criminalised if any of those acts are for the purposes of sexual exploitation of the child. An attempt to commit any of the acts, or complicity or participation in any of the acts must also be covered under the criminal law of the ratifying states.

The actions are covered under the Protocol whether they are committed domestically or transnationally, or on an individual or organised basis.





WHAT ARE THE MAJOR LEGAL ISSUES?



Differences in Laws

One of the most difficult aspects of prosecuting the sexual exploitation of children on the Internet is the difference between laws in different countries. Countries differ on their definitions of children, on what pornography is, on what forms it can take and on whether an overt act—or merely an intention—is needed for prosecution. They also differ on whether simple possession is a crime or whether a real child had to be involved. Without harmonisation of laws, offenders will continue to seek shelter in jurisdictions that have limited child abuse and child pornography laws.



For instance, not until 18 July 1999, did Japan finally enact a law that defined child pornography and prohibited its distribution, sale and display. A study by the German police of hotline complaints found that 81% of complaints to hotline homepages could not be dealt with because no German or foreign law was broken. Fifty percent of the Internet related cases referred to German hotlines called for investigation abroad.¹



While legislation needs to be harmonised between countries in order to ensure that child abuse and child pornography can be prosecuted worldwide, the most important thing is to utilize existing laws to deal with criminal activities involving children on the Internet. The pace at which technology is developing may quickly make Internet-specific laws outdated.



¹ *Combating Child Pornography on the Internet, Holder Kind, International Conference Combating Child Pornography on the Internet, Vienna. 29 September - 1 October, 1999.*



Jurisdiction

Even though the Internet is international, the authorities that control activities on the Internet are national. Sometimes they only are empowered at the state level.

Jurisdiction for international activities can operate in a number of different ways. It may operate in relation to where an offense was committed or where the damage occurred. The transmission of child pornography over the Internet often poses jurisdictional problems because it may be impossible to establish where the material came from or where the damage occurred.

In child abuse or exploitation cases, some jurisdictions and laws require the offender to be present in the jurisdiction, while others require both that the offender be in their territory and that the offense occurred there. Yet other jurisdictions and laws require that only the minor victim be present on their territory.

Legislation in many countries, however, has made it possible to prosecute nationals for offenses against children which occur outside those countries' territorial boundaries. Some countries have devised special legislation to deal with the jurisdictional problems related to illegal and harmful uses of the Internet. New Zealand imposes strict liability for possession of child pornography, thus avoiding difficult matters of proof of intent or origin.

The Council of Europe has introduced an International Convention on CyberCrime. The Convention is open for ratification by all European Council member states and non-member States which have participated in the conventions' elaboration. At least within Europe, this will answer some of the problems of jurisdiction and make judicial co-operation between European countries faster and simpler.





Forms

While in most countries general laws on pornography also apply to child pornography, in some countries pornography is defined only for visual mediums. Sound, CDs with text or audio are not deemed to be pornographic. Also, real time transmission of images across the Internet is a form which was not invented when most laws were written.

It is hoped that instruments such as the Optional Protocol and European Cybercrime Convention will answer the problem of the different forms of Legislation in each state by defining the most important elements of the offence.

Child Pornography is defined in the protocol as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes”.

Child Pornography is defined in the European Cybercrime Convention as “ 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.”

It is hoped that most states will ratify the Protocol and Convention in entirety so that a minimum level of protection will be universally available.

Why is Criminalising Possession Important?

Making the mere possession of child pornography a criminal offense is important for several reasons. Sometimes the police are not sure if a child has been sexually abused. Finding pornographic images of that child will confirm that abuse did take place.

Often child pornography found in searches of houses, offices or computers will lead police to missing children. Finding child pornography can also provide the evidence to convict a child abuser who has evaded detection.



Some people have argued that just having child pornography should not be an offense. But the fact is that for every pornographic image of a child, an offense has been committed against that child. The possessor of the image is like the receiver of stolen goods. If he did not provide the 'market' for the record of the abuse, the abuse would not have occurred. Also, specialists who work with child abusers say that people who possess pornographic images of children are either abusers themselves, or would like to be child abusers. Possession should therefore only be permitted for judicial or police authorities.



Who Is A Child?

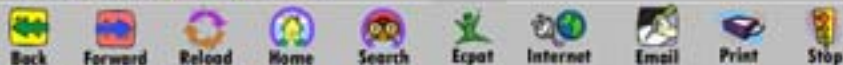
Despite the fact that the Convention on the Rights of the Child defines a child as anyone below the age of 18, the definition of a child varies widely between countries and even between states within federally-constituted countries. Children can be defined by age or by sexual maturity. Most definitions of children set the legal age between 13 and 18. In some jurisdictions it is not necessary to determine the age of the child to prosecute child pornography cases. In these jurisdictions, it is sufficient that the impression of a child was created.

The definition of Child Pornography contained in the Optional Protocol and the European Cybercrime Convention includes not only images of real minors but images of persons appearing to be or representing minors.

What Aspects of Pornography Are Criminalised?

Among the aspects of child pornography which are criminalised are possessing, stocking, selling, distributing, exporting, importing, intending to distribute, intending to depict or encourage child abuse, supplying, or aiding or abetting any of the above. Whether or not payment is made can be important in some jurisdictions, but not in others. In some countries, Internet-specific laws dealing with child pornography have been introduced.





WHAT ABOUT FREEDOM OF EXPRESSION?

There are people who argue that their right to freedom of expression gives them the right to possess child pornography and to exchange and discuss it with other people. While freedom of information is necessary to ensure the greatest dispersion of views on the Internet, the sexual abuse of children, child pornography and paedophilia is unacceptable in any community, whether it occurs in real-life or on-line. Societal values do not change simply because technology has advanced.

Freedom of expression is not an absolute right. The U.N. International Covenant on Civil and Political Rights outlines several rights to which there can be no restriction or derogation, but the right to freedom of expression is not one of them. In fact, Article 19 provides for the right to freedom of expression in this way:

Everyone shall have the right to hold opinions without interference.

Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

The exercise of the rights provided carries with it special duties and responsibilities.

...may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

For respect of the rights or reputation of others;

For protection of national security or of public order, or of public health and morals.

This provision shows that freedom of speech, in international jurisprudence, is not absolute, and must be balanced against the right of children to be protected from sexual abuse and invasion of their privacy.



FIRST AMENDMENT AND MORPHING CONCERNS IN THE UNITED STATES

In April 2002, the United States Supreme Court found that provisions of the Child Pornography Prevention Act (CPPA), which prohibited the depiction of virtual and simulated child pornography, were invalid under the First Amendment of the United States Constitution which protects freedom of speech.

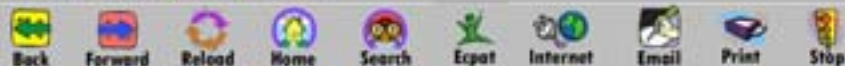
Supporters of the CPPA argue that virtual and simulated child pornography are not only used by child sex abusers to solicit victims, but by that the very existence of these images whets the appetite of child sex abusers and encourages them to seek out new child victims.

The US Supreme Court however found that in the absence of the depiction of a “real” child they could see no “direct link” between such images and the sexual abuse of children. The majority of Justices also said that they could see no substantial risk of producers of child pornography using virtual images of children.

The majority of the Court believed that the CPPA may have effectively banned speech that had “serious literary, artistic, political or scientific value”. The majority gave the example of “Romeo and Juliet” a love story that involves sexual intimacy between two fourteen year olds. The story has been filmed and acted many times with actors older than 14 playing the lead roles. However, a minority of the Supreme Court believed that this was an exaggeration of the powers contained in the CPPA. They pointed out that despite the CPPA being in effect since 1996, Hollywood had produced many films exploring teenage sexuality, such as Traffic and American Beauty, these film makers were never prosecuted under CPPA nor did they stop making the films because of the existence of the CPPA.

US Attorney General John Ashcroft stated that although he was disappointed with the decision it would inspire the Justice Department to redouble their efforts to investigate and prosecute child pornography cases, he also pledged his commitment to work with the United States Congress to develop new laws that would pass court scrutiny.





FREEDOM OF EXPRESSION?

John Sharpe, a retired Canadian city planner, was caught with photos of nude boys and pornographic short stories involving children. He represented himself, and successfully fought in two courts a charge of possession of child pornography on the grounds that Canadian child pornography laws intruded into his right to freedom of expression and his right to privacy. In January 2001, those decisions were appealed to the Supreme Court of Canada. ECPAT International and two of its' Canadian affiliates were allowed to make submissions to the Supreme Court.

The Criminal Code of Canada section 163.1 contained a broad definition of Child Pornography which extended to “visual representations” and “written material” that advocated or counselled sexual activity with a person under 18 years of age.

The Majority of Judges of the Supreme Court of Canada held that the harm caused to children by child pornography justified criminalising the possession of some forms of child pornography despite the fact that this infringes a person’s right to freedom of expression.

The Judges then focused on two specific forms of Child pornography that were prohibited by the legislation: 1) written material or visual representations created and held by the accused alone exclusively for personal use; and 2) visual recordings created by or depicting the accused that do not depict unlawful sexual activity and are held by the accused exclusively for private use. The judges said that this aspect of the legislation went too far. They held that the cost to freedom of speech outweighed “any tenuous benefit it might confer in preventing harm to children”.

Thus, although the decision confirmed the right of the government to criminalise the mere possession of child pornography, it limited the right of the government to prescribe what type of child pornography could be prohibited.

On March 26, 2002 John Sharpe was found guilty of two charges of possession of child pornography. However, he was found not guilty of a further two charges relating to his writings. The Court found that stories written by Sharpe entitled “Sharpe’s Kiddie Kink Classics”, “Tijuana Whip Fight” and “Suck It” did not advocate the commission of sex crimes against children and had some artistic merit. On 2 May 2002, Sharpe was sentenced to four months house arrest that included electronic monitoring for 16 hours a day, a prohibition on contact with people under 18 and strict supervision of his Internet usage.

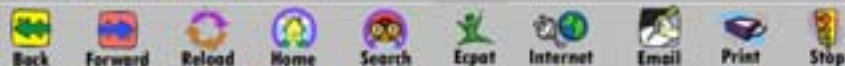


Protecting Children

WHAT CAN PROTECT CHILDREN ON THE INTERNET?

Parents need to be involved with their children's Internet experience. Teaching children how to handle themselves on the Internet is important. There are also filtering software packages and web site rating schemes designed to help parents guide their children's Internet experience while still allowing that child Internet independence.





Awareness: NetSmart Rules

In many countries, ECPAT groups and other organisations have already begun awareness raising programmes with young people and adults about being safe on the Internet.

Among the Internet usage rules for children which these programmes promote are the NetSmart rules:¹

- Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, unless your parent or carer specifically gives you permission.
- Never send anyone your picture, credit card or bank details, or anything else, without first checking with your parent or carer.
- Never give your password to anyone, not even a best friend.
- Never arrange to meet anyone in person without first clearing it with your parent or carer, and get them to come along to the first meeting, which should always be in a public place.
- Never hang around in a chat room or in a conference if someone says or writes something which makes you feel uncomfortable or worried, and always report it to your parent or carer.
- Never respond to nasty, suggestive or rude e-mails or postings in Usenet Groups.
- Always tell your parent or carer if you see bad language or distasteful pictures while you are online.
- Always be yourself and do not pretend to be anyone or anything you are not.
- Always remember if someone makes you an offer which seems too good to be true, it probably is.

¹ See NCH Action for Children: www.nchafc.org.uk

HOW DO FILTERING AND RATING SOFTWARE PACKAGES WORK?

Filtering Software

Rating and filtering software is designed to identify content which might be harmful to younger viewers. The software allows parents and guardians stop children from coming across sites which they consider harmful. It is not meant to interfere with freedom of expression, or prevent adults from viewing anything they wish to see.

Rating and filtering software should be culturally neutral, in order that each user can apply their individual standards and national culture. The software also needs to be cheap and simple to use, so that even parents with limited computer skills can install it.

The first filtering software was quite unsophisticated and based on key words, which basically could not differentiate between pornographic and medical sites. Recent software is much improved. Some use automated programs called “spiders” which crawl across the Internet and investigate what is on sites. Other programs use real people searching out sites and determining their content. Both types of programs usually put web sites into categories to which access can be forbidden. Much software, however, still cannot screen for explicit images unless it is accompanied by text or unless the site has been visited and marked by a filtering rater.

Filtering software follows three main models; blacklisting, whitelisting and neutral labeling. Blacklisting blocks access to listed sites, whereas whitelisting allows access only to listed sites, blocking all the others. In neutral labeling the sites are labeled or rated, but it is up to the user to decide how to use the rating system.

Blacklisting technique is used, for instance, in Cyber Patrol’s software. Cyber Patrol has grouped





approximately 10000 sites into twelve categories, of which parents can selectively choose the groups they want to be blocked.



In whitelisting, access is blocked to any site except ones the user has specifically designated. This technique is very limiting, but it is very safe and a good choice especially when there are very young children using the Internet.

Rating Software



Rating systems utilize descriptions of a web site's content. Ideally, rating systems should be objective, having no reference to national or cultural values or opinions. Users themselves should be given the choice to make subjective judgments on the level of rating. Internet rating systems, however, cannot be applied to chat rooms or video conferencing, which are ever changing and contain no static content which can be rated.



PICS

Most rating systems are based on the Platform for Internet Content Selection (PICS), developed by the World Wide Web Consortium, a group of Internet leaders founded to develop common protocols to enhance the interoperability and lead the evolution of the World Wide Web. PICS is a set of technical specifications that help software and rating services to work together, but PICS itself is neutral.



PICS works by embedding electronic labels in the text or image documents which allows rating software to vet the document's content before the computer displays them or passes them on to another computer. PICS tags can be added by the publisher of the material, by the company providing access to the Internet, or by an independent vetting body.



There are several rating systems which use PICS:



- The Recreational Software Advisory Council (RSAC) runs RSACi (RSAC on the Internet), a system which rates sites on the Internet. (www.rsac.org). The rating system is similar to the one used to rate computer game violence, nudity, vulgarity etc. Parents can select the type of content and levels of rating appropriate for their children.

- A new, global ratings system based on the RSACi system has been formulated by a body called ICRA (Internet Content Rating Association), which in turn has benefited greatly from the work of INCORE (Internet Content Ratings for Europe) an EU-funded project organized by the UK's Internet Watch Foundation. INCORE carried out a feasibility study into the possibility of establishing a new European-wide rating system which, while improving on the RSACi model, would be more in tune with Europe's different cultural and linguistic needs. The new system can be used with Microsoft's Internet Explorer immediately, with wider applications under development. The existing RSACi labels can continue to be used in both Internet Explorer and Netscape Navigator but will be phased out over time.

- SafeSurf uses more rating categories than RSACi, having its own rating standards. It has many locations mirrored around the web where web site operators can fill out the questionnaire for a rating. In each category there are nine levels, based strictly on age.

Self-rating

In self-rating the content providers submit information about their sites and are given a rating code for their site. Rating is done by the content providers themselves, but the organisations providing the system reserve the right to confirm the accuracy of the rating. Voluntary self-rating should be encouraged, since it can create a "virtuous circle", meaning that the more rating software is used by the Internet users, the more content providers start to rate their sites, making it more attractive to use rating software, and so on.

ISP Filtering

Filtering software can also be installed by an ISP. If the service providers control filtering, they may become liable for any illegal content which gets through, while the user must rely on others to make decisions about the content. If the filtering is by the user himself, then he has personal control over the content filtered, and liability remains with the content provider. ISP-based filtering is growing in popularity, especially in the USA, where several religious organisations have established their own systems. Similar services also exist in the United Kingdom and Germany.





WHAT IS BEING DONE NOW?



Because of the nature of the Internet, widespread cooperation is needed between officials in many jurisdictions. Hotlines and ISP codes of conduct help with reporting and removal of child exploitation web sites. Hotlines often work with local and international law enforcement organisations, including various customs organisations and Interpol.

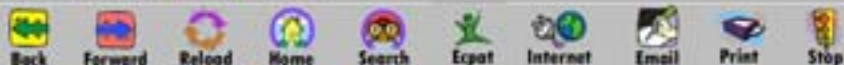
Hotlines

Hotlines receive reports from the general public about child exploitation web sites, newsgroup postings and child exploiters via internet, phone, print, fax, mail. Hotlines can have great success in fighting child pornography and child abusers. Between the launch of the Internet Watch Foundation's hotline in December, 1996 and the end of 1999 hotline tips caused over 20,000 items to be recommended for removal from ISPs in the United Kingdom.

Hotlines provide the public with advice on how to pursue a complaint against an offending website. Hotlines can also ask a poster to remove offending content and advise ISPs to remove the content. In addition, law enforcement may be advised, and content from another country dealt with by passing information to another hotline or relevant law enforcement agency. Information often moves faster through hotlines than through such agencies.

Hotlines also encourage, promote and assist in the development of rating systems. They disseminate information about the hotline service to Internet users. All good hotlines are transparent in their workings, and report in an open manner on their operations.

The Internet Hotline Providers Europe (INHOPE Association) encourages and supports new hotlines, and is working towards ways in which hotlines can cooperate effectively. The ultimate aim is to have a European network of hotlines.



For an international network of hotlines to function effectively, they would need a framework agreement containing minimum standards on the handling of content concerns and stipulating mutual notification. The hotline in the country where the content is located must evaluate it and take action. This mechanism ensures that action is taken where the content is illegal.¹

ISP Codes of Conduct

In several countries, ISP associations have drafted codes of conduct in order to clarify their roles and responsibilities relating to the illegal content on the Internet. For instance, EuroIspra brings together European Internet service providers associations. Its members come from ten European countries: Austria, Belgium, Finland, France, Germany, Ireland, Italy, the Netherlands, Spain and the UK, representing 500 service providers.

The European Council Recommendation on the Protection of Minors and Human Dignity in Audiovisual and Information Services provides several points that should be taken into account in the process of drafting a code of conduct for ISPs:

- Users need to be informed of basic rules for internet usage, and of the legal responsibilities of those providing content
- Minors should be protected from harmful content
- Protection measures, such as a warning page, visual or sound signal, labeling or classification or systems to check the age of users should be used when potentially harmful content may be available
- ISPs should provide support for parental controls such as filtering software
- A way to handle complaints should be instituted
- ISPs should support effective measures in the fight against illegal content offensive to human dignity
- Basic rules of cooperation between operators and judicial and police authorities should be spelled out for ISPs
- Procedures should be included for dealing with violations of the codes of conduct.

¹ Key Recommendations: Internet Content Summit, Bertelsmann Foundation, Germany, 1999.





Different national codes emphasize different aspects of an ISP's responsibilities. The Italian code of conduct focuses on three main points relating to self-regulation of ISP activities: liability, identification and anonymity. Responsibility lies with the person who provides content on the Internet. The Italian code also calls for the ability to trace content providers and verify their identity in order to establish liability. At the same time, however, Italy's code emphasizes the privacy of individuals and the importance of protecting anonymity, taking into account the balance between preserving anonymity and providing help to law enforcement officials in their efforts to trace illegal content.



According to the British code of conduct, members of the UK ISPA, after receiving a notice from the Internet Watch Foundation (IWF) requesting prompt removal of specified material from web sites or newsgroups, must comply with such notices within a reasonable time and simultaneously inform the originator of such material, provided the content provider is their customer.



In the United States of America, several large communications companies including America on Line and AT&T have joined together to provide a Get NetWise Safety Service. They provide safety tips for all ages, a Neighbourhood Watch system, and law enforcement information.





How Software Helps Combat Exploitation

While new technologies and software have given child exploiters new tools, it has also provided law enforcement agencies with means to improve their investigations. Germany now has a compound database which stores data about pornography, including email addresses and nick-names of producers, distributors and collectors.¹

In addition, the German police have also created a database of over 50,000 images of child pornography gleaned from the Internet. Most of these photos are over a decade old; new child pornography is often initially distributed to a limited audience. From this database, the German police have extrapolated that at least 300-350 children were sexually assaulted and photographed to make these images.

Among other plans suggested have been a cross-checking system to see if child pornography seized in one country is already on file in another, and linking pornographic images to previously documented criminal case files.



¹ *Combating Child Pornography on the Internet*, Holder Kind, International Conference Combating Child Pornography on the Internet, Vienna. 29 September-1 October, 1999.



WHAT CAN YOU DO?

Individuals and groups can help fight the use of the Internet in the exploitation of children in a number of ways by:

Better laws:

Zero tolerance on child pornography!
Lobby your local elected representative to make sure that the legislation in your country is adequate i.e. that it criminalises production, distribution and even mere possession of child pornography and make sure there is a good definition of what 'child pornography' means in your legislation and that it covers pseudo child pornography (morphed pornography).

Seek the highest possible standards for child protection in your national legislation.



Harmonisation of laws:

Encourage your legislators to discuss legislation at regional and at international level to ensure the greatest possible level of legislative harmonisation between countries. Campaign for the adoption and then the ratification of the Optional Protocol and the Convention on CyberCrime.

Law Enforcement:

Promote the establishment in your country of specialised police units dedicated to combating the criminal use of the Internet. Such units need training and high performance computer equipment.

Encourage the exchange of technical expertise and training for 'cyber-cops'. Encourage police units to develop contacts with their foreign counterparts so that they can gain from the technical know-how of others and learn how to track and find child abusers.



Japanese Police Agency - Supporting the Protection of Children Online

In March 2002, ECPAT/STOP Japan released the 1st Japanese edition of "Protecting Children Online: An ECPAT Guide". A representative of the National Police Agency was among those who spoke at the launch.

Japan only enacted laws specifically combating commercial sexual exploitation of children through pornography in November 1999. For a country who does not have a long history of a comprehensive legislative programme in combating child pornography it is extremely encouraging that the Japanese Police Agency has ordered an entirely new reprint of "Protecting Children Online" to assist in the training of their police officers.





ISPs:

Make sure that your local ISPs have a Code of Conduct about child pornography. Encourage your local ISPs to cooperate with the police and with each other on this issue.

AUSTRALIA

Australia recently passed the Broadcasting Services Amendment (Online Services) Bill 1999¹, which clarifies the responsibilities of the ISPs relating to prohibited content. The Act excludes ordinary email and chat services. For purposes of controlling child pornography, a child is defined as a person who is or looks like a person under 16 years.²

The Bill came into effect on January 1, 2000, and faced strong criticism in Australia, since it does not only cover illegal content, but also offensive and X-rated material. This law does not make ISPs legally responsible for content hosted on their servers, unless they fail to remove the content once they become aware of it. Not knowing about illegal content hosted on their servers does not create criminal liability.

Individuals can issue complaints to the Australian Broadcasting Authority (ABA) about content on the Internet via their web site or via fax, letter or phone. ABA will then give a notice to the ISP or the content provider, provided it considers the content to be prohibited (this judgment is made based on a law relating to conventional media). The ISP has to remove or block the access to the content in a given time from the notice. If the content originates from abroad, the ISPs have to take "reasonable steps" based on their code of Conduct to block access. The Australian police are notified of the content in order to inform the relevant authorities abroad.

Hotlines:

Support your local Hotline (See the list on page 49) or encourage the establishment of a national specialist Hotline. Maybe your local ISPs would do this.

If necessary, set up your own Hotline. Encourage networking between Hotlines.

In any event, **REPORT THE PRESENCE OF CHILD PORNOGRAPHY** to the appropriate authorities.

¹ For the complete text of the bill, see <http://scaleplus.law.gov.au/html/comact/10/6005/top.htm>.

² Approaches to Establishing New Hotlines - An Australian Perspective, Gareth Grainger, International Conference Combating Child Pornography on the Internet, Vienna, 29 September-1 October, 1999.



Hotlines - assisting law enforcement to crack down on on-line pornography rings

On 16 January 2001, Sweden's largest child pornography ring involving more than 50 suspects was broken after Police were tipped off by the Save the Children organisation. The Save the Children organisation, was notified of the material by a caller to its hotline in November 2000 and reported it to the police.

Material found in the confiscated computers contained pornographic pictures and video clips of "children of all ages, some very young," the Swedish Police said.

Spreading child pornography, is a crime under Swedish law that can lead to prison sentences of up to four years.

Tips on setting up a hotline

- Involve the national authorities from the beginning and during the whole process.
- Involve and communicate with the Internet Service Providers operating within the Hotline's area of responsibility. The Hotline needs their acceptance, trust and support during its day to day work.
 - Concentrate the Hotline's responsibility on well-defined areas of law. Avoid areas where the Hotline could be accused of trying to apply censorship.
 - Have clearly defined, well understood and openly accessible procedures.
 - Gather experience from existing institutions working in similar areas.
 - Inform Internet users about the service, using all available means of communication.

** Adapted from the paper by Karl Hirschmann of ISPA to the International Conference on Combating Child Pornography on the Internet, Vienna, Sept. 1999.*





At home:

Learn to use a computer! Know what your children are doing on-line. Take responsibility as a parent or carer to make sure that your computer-kid is 'NetSmart'. (See the rules on page 30)

Buy or make sure your computer has filtering software.



Campaigns that involve parents

Accion Contra la Pornografia Infantil (ACPI), an ECPAT affiliate in Spain launched a campaign in 2000 called 'Jugar Tranquilo'. Parents are taught to recognise symptoms of child abuse and the methods by which paedophile abusers operate, including through the Internet.

Also in 2000, ECPAT Taiwan organised and trained voluntary teams of parents to handle the reports received on their hotline (Web 547) and instructed them on how to monitor their children's use of the Internet.

At school:

Make sure that the local school is providing the necessary skills to pupils so that they will understand the benefits and the limitations of on-line information.

Distribute the 'NetSmart' rules in school.





New Zealand Internet Safety Group and the Ministry of Education

The New Zealand Ministry of Education worked in conjunction with other government departments, schools and NGO's, including ECPAT to develop an Internet Safety Kit for distribution in schools.

The Kit includes an "Internet Safety Agreement" that is signed by a child and their guardian to ensure families work together to keep internet usage safe. The Kit also includes practical tips and hints for parents, teachers and children on how to have fun on-line without jeopardising a child's safety.

You can view an on-line version of the kit at :-
<http://www.netsafe.org.nz/ie/kit/index.asp?xmldata=kit.xml>

ACPI, the ECPAT affiliate in Spain, will continue its work with Internet Safety through a new campaign in 2002. This campaign is being carried out in cooperation with the Children's Ombudsman and one of the largest Internet Service Providers for Spanish sites, Terra-Lycos. For the campaign, ACPI has created an 8 page comic book for young people that explains basic rules that should be followed when using the Internet. Mouse pads for all school computers, with illustrations reminding users of these rules, and an informative brochure for parents will be distributed at the same time. Terra-Lycos is creating 'safe zones' with sites that are appropriate for young surfers and installing content filtering software on school's servers.



Content



Internet



Dangers



Legal issues



Protect children



Resources



Appendices



Additional Reading



- Carr, John. Child Pornography (theme paper prepared for the Second World Congress). ECPAT International; 2001. http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf



- Commission of the European Communities. Communication From the Commission to the Council and the European Parliament on Combating Trafficking in Human Beings and Combating the Sexual Exploitation of Children and Child Pornography. Brussels; 2000. http://europa.eu.int/comm/avpolicy/regul/new_srv/ermin_en.pdf



- Greenfield, Paul; Rickwood, Peter, and Tran, Huu Cuong. Effectiveness of Internet Filtering Software Products. NetAlert and the Australian Broadcasting Authority; 2001. www.aba.gov.au/internet/research/filtering/index.htm



- Hecht, Mark. The Role and Involvement of the Private Sector (theme paper prepared for the Second World Congress). ECPAT International; 2001. http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_private_sector.pdf



- Klain, E. et al. Child Pornography: The Criminal Justice System Response. USA: National Center for Missing and Exploited Children; 2001. www.missingkids.com/download/NC81.pdf
- Machill, Marcel and Rewer, Alexa. Internet-Hotlines: Evaluation and self-regulation of Internet content. Germany: Bertelsmann Stiftung; 2001.
- O Connell, Rachel. Untangling the complexities of combating paedophile activities in cyberspace. University of Central Lancashire, Cyberspace Research Unit; 2000.



- Quayle, Ethel and Taylor, Max. Child pornography and the Internet: Perpetuating a cycle of abuse. Ireland: COPINE Project, Department of Applied Psychology, University College Cork; 2001.
- Williams, Nigel. Are we Failing our Children?- An assessment of Internet Safety Initiatives. Childnet; 2001. <http://www.childnet-int.org/publicat/singapore.html>

Online Links

Education

- Action for Children in Cyberspace (US) (<http://cme.org>)
- Global Chalkboard (<http://www.bascom.com/html/solutions/gcb/globalchalkboard.htm>)
- kIDsAP (<http://www.kidsap.org/>)
- Missing : An educational kit about Internet kidnapping (<http://www.livewwwires.com>)

Action Groups

- The Anti Pedophile Network (<http://hotstreak.net/anti/>)
- The Bertelsmann Foundation (<http://www.stiftung.bertelsmann.de/internetcontent>)
- Casa Alianza (<http://www.casa-alianza.org>)
- Child Rights Information Network (CRIN) (<http://www.crin.org>)
- Childnet International (<http://www.childnet-int.org>)
- Defense for Children International (<http://www.defence-for-children.org/>)
- ECPAT International (www.ecpat.net)
- Enough is Enough (<http://www.enough.org>)
- Focal Point Against Sexual Exploitation of Children (<http://www.focalpointngo.org/>)



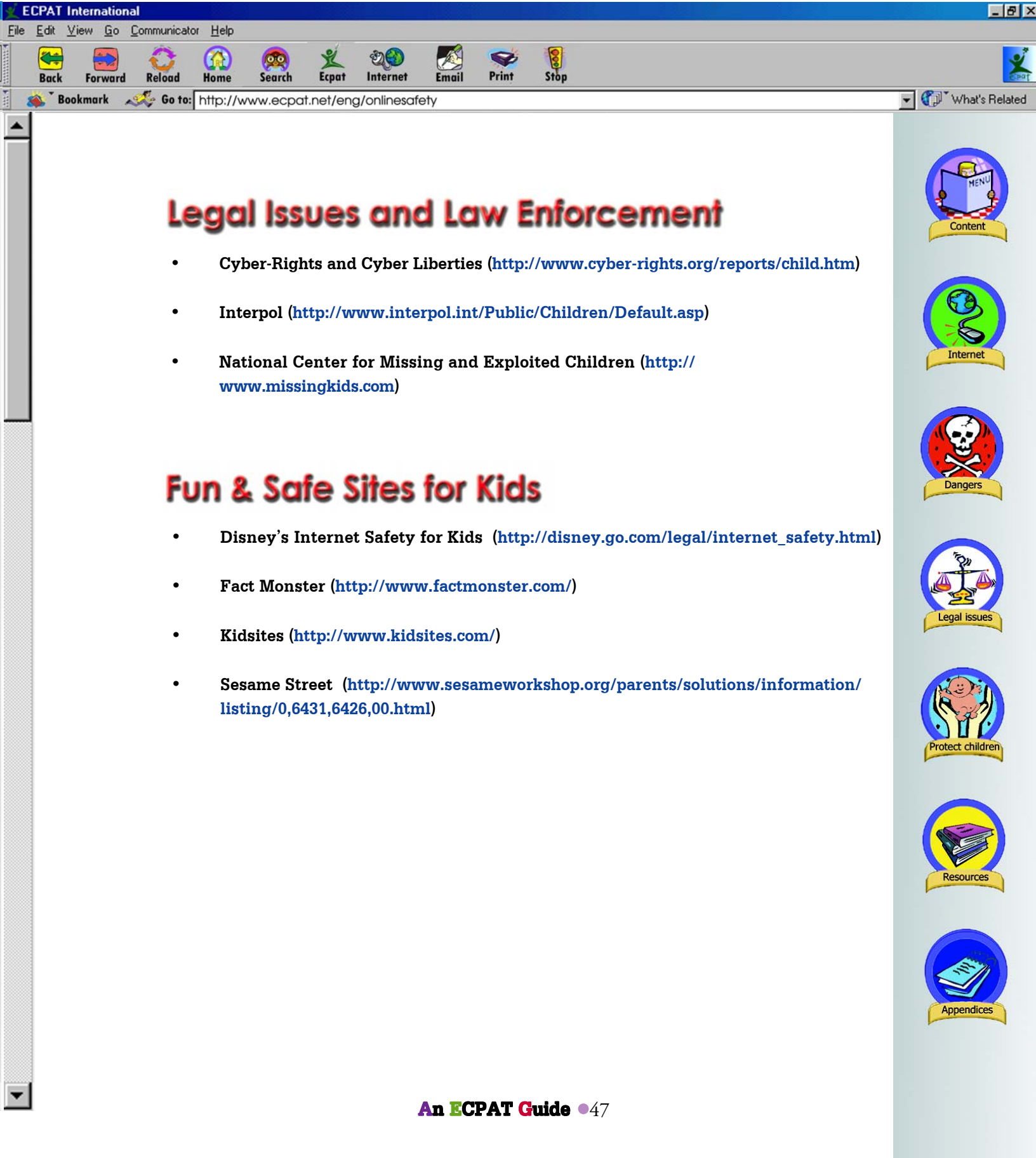


- **INCORE - Internet Content Rating for Europe** (<http://www.incore.org>)
- **Innocence in Danger (UNESCO)** (<http://www.unesco.org/webworld/innocence>)
- **International Bureau of Children's Rights** (http://www.ibcr.org/programs_en.shtml)
- **Internet Watch Foundation** (<http://www.iwf.org.uk>)
- **NCH Action for Children (UK)** (<http://www.nchafc.org.uk/home.html>)
- **Netaware – Safe use of the Internet (an EU Awareness Project)** (<http://www.netaware.org>)
- **New Zealand Internet Safety Group** (<http://www.netsafe.org.nz/ie/kit/index.asp?xmldata=kit.xml>)
- **PedoWatch – Monitoring Paedophilia on the Internet** (<http://pedowatch.org/pedowatch/>)
- **UNICEF** (<http://www.unicef.org/crc/oppro-frameset.htm>)
- **Wired Patrol** (<http://www.cyberangels.org/>)



Government Links

- **Australian Broadcasting Authority (ABA)** (<http://www.aba.gov.au>)
- **European Union** (http://www.europa.eu.int/information_society/programmes/iap/index.en.htm)
- **Eurochild** (<http://www.eurochild.gla.ac.uk>)



Legal Issues and Law Enforcement

- Cyber-Rights and Cyber Liberties (<http://www.cyber-rights.org/reports/child.htm>)
- Interpol (<http://www.interpol.int/Public/Children/Default.asp>)
- National Center for Missing and Exploited Children (<http://www.missingkids.com>)

Fun & Safe Sites for Kids

- Disney's Internet Safety for Kids (http://disney.go.com/legal/internet_safety.html)
- Fact Monster (<http://www.factmonster.com/>)
- Kidsites (<http://www.kidsites.com/>)
- Sesame Street (<http://www.sesameworkshop.org/parents/solutions/information/listing/0,6431,6426,00.html>)



Content



Internet



Dangers



Legal issues



Protect children



Resources



Appendices



Content



Internet



Dangers



Legal issues



Protect children



Resources



Appendices

Internet Blocking, Filtering & Usage Tracking Software

- BESS (www.bess.net)
- Children's Internet Browser (<http://www.chibrow.com>)
- Cyber Patrol (www.cyberpatrol.com)
- Cyber Sentinel from Security Software Systems (www.securitysoft.com)
- Cyber Snoop (www.pearlsw.com)
- CyberSitter (www.cybersitter.com)
- Global Chalkboard (www.bascom.com)
- KidDesk (www.edmark.com/prod/kdis/)
- N2H2 (www.n2h2.com)
- Net Nanny (www.netnanny.com)
- Net Shepherd (www.netshepherd.com)
- Recreational Software Advisory Council (www.icrq.org)
- Safe Surf (www.safesurf.com)
- Surf Monkey (www.surfmonkey.com/default.asp)
- Parents' Internet Resource Center (<http://parents.surfmonkey.com>)
- Corporate Website (<http://kids.surfmonkey.com/company/default.asp>)
- Surf Watch (www.surfwatch.com)
- The Internet Filter (www.turnercom.com/if/index.html)
- X-stop (www.xstop.com)

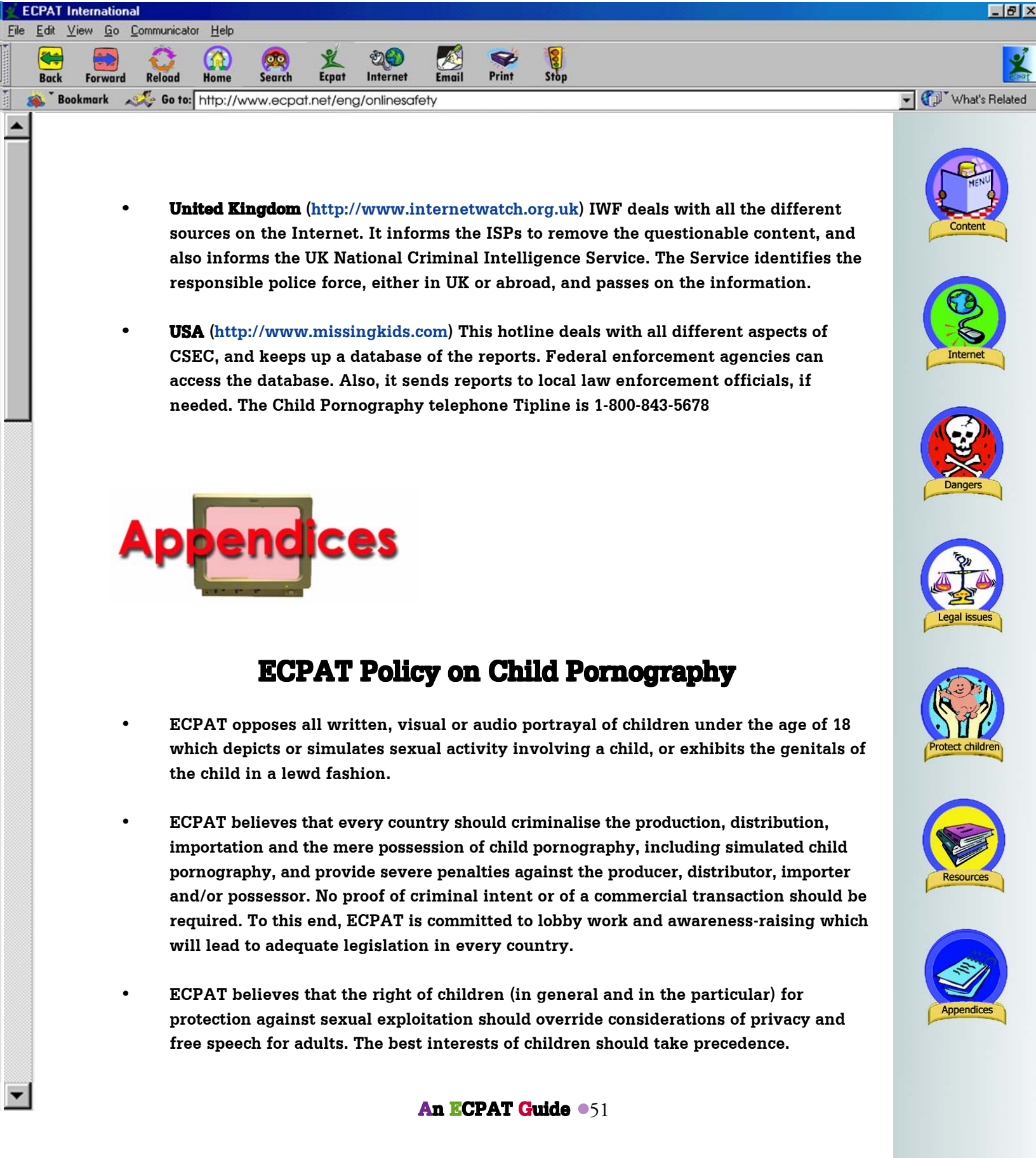
Hotlines

- **Australia** (<http://www.aba.gov.au/internet/complaints/complaints/complaints.htm>) Internet sites and newsgroups containing child pornography or other offensive material can be reported. NetAlert, a telephone and Internet service to offer advice to children and families on safe use of the Internet.
- **Austria** (<http://hotline.ispa.at>) The Austrian hotline focuses on child pornography and neo-nazis. It informs the content provider and asks for removal of the illegal content, unless the content originates from abroad, in which case it informs the relevant authorities. Also, it informs other European hotlines.
- **Brazil** (<http://www.violenciasexual.org.br/>) This hotline is operated by Centro de Defesa da Criança e do Adolescente in Bahia (CEDECA-BA). CEDECA BA shares a common database with the Federal Police, thereby eliminating dual reports. Reports can be made on sexual violence in general, or specifically on child pornography on the Internet.
- **Finland** (<http://www.poliisi.fi>) This hotline service is operated by the National Bureau of Investigation. E-mail: vihje.internet@krp.poliisi.fi
- **Finland** (<http://www.mll.fi>) The Children's Ombudsman of the Mannerheim League for Child Welfare operates a hotline and legal advisory service on child pornography and paedophilia activities.
- **Germany** (<http://www.fsm.de>) FSM only deals with content originating from Germany, and does not cover Usenet news or IRC. It does not pass complaints to the police, but rather works through recommendations for removal of the questionable content.





- Germany** (<http://www.eco.de>) Reports can be made about illegal content on websites, newsgroups, discussion forums, etc. The hotline informs ISPs if content is considered illegal and does not distinguish between content that is local or originates from abroad. ECO does not pass the information to the police.
- Ireland** (<http://www.hotline.ie>) The hotline receives reports from Ireland and abroad and concentrates exclusively on child pornography and sexual exploitation of children. It covers www and newsgroups, but IRC only to a limited extent. The content of a report is evaluated, and if considered illegal under Irish law and located on a server in Ireland, the police and the ISP are both notified. The relevant foreign hotline is notified for reports of material hosted outside of Ireland.
- Netherlands** (<http://www.meldpunt.org>) Meldpunt was the first hotline for reporting child pornography on the web, set up in Holland in 1996. Staff inform the police, in the case that the content provider does not remove the illegal content within 24 hours of the warning given by Meldpunt. Hotline staff also inform the ISP, asking it to give assistance to the police, if necessary.
- Norway** (children@risk.sn.no) It receives reports both from Norway and from abroad, and concentrates specifically on child pornography and sexual exploitation of children. It covers www, Usenet news, IRC etc, and passes the information to the police, but does not contact the content provider nor the ISPs, except when an ISP provides access to a range of illegal material, e.g. a particular newsgroup focusing on paedophilia.
- Spain** (<http://www.protegeles.com>) This hotline is operated by OPTENET and ACPI, an ECPAT affiliate, and is focused specifically on reports about child pornography on the Internet. They accept reports from anywhere in the world. Staff inform the Spanish police or the police of the country from which the pornographic page originates.
- Taiwan** (<http://www.web547.org.tw>) The first Chinese language web-based hotline (Web 547) was launched by ECPAT Taiwan In 1999. It allows visitors to report sites with pornographic or indecent material.



- **United Kingdom** (<http://www.internetwatch.org.uk>) IWF deals with all the different sources on the Internet. It informs the ISPs to remove the questionable content, and also informs the UK National Criminal Intelligence Service. The Service identifies the responsible police force, either in UK or abroad, and passes on the information.
- **USA** (<http://www.missingkids.com>) This hotline deals with all different aspects of CSEC, and keeps up a database of the reports. Federal enforcement agencies can access the database. Also, it sends reports to local law enforcement officials, if needed. The Child Pornography telephone Tipline is 1-800-843-5678

Appendices

ECPAT Policy on Child Pornography

- ECPAT opposes all written, visual or audio portrayal of children under the age of 18 which depicts or simulates sexual activity involving a child, or exhibits the genitals of the child in a lewd fashion.
- ECPAT believes that every country should criminalise the production, distribution, importation and the mere possession of child pornography, including simulated child pornography, and provide severe penalties against the producer, distributor, importer and/or possessor. No proof of criminal intent or of a commercial transaction should be required. To this end, ECPAT is committed to lobby work and awareness-raising which will lead to adequate legislation in every country.
- ECPAT believes that the right of children (in general and in the particular) for protection against sexual exploitation should override considerations of privacy and free speech for adults. The best interests of children should take precedence.





- ECPAT supports the search for suitable model legislation and law enforcement mechanisms, including bilateral and multilateral arrangements to ease the prosecution of Internet-related use of child pornography. ECPAT seeks to develop positive and co-operative relationships with Internet Service Providers (ISPs) and with the software and search engine production industries in order to find solutions to the technological problems concerning the transmission of child pornography via computer and the Internet.
- ECPAT encourages the ISPs to develop appropriate Codes of Conduct which will include a commitment to the reporting of child pornography to the police, and give notice to users of that intention, as well as the development of child-friendly information on their sites. ECPAT encourages the ISPs to give all possible support to law enforcement agencies to prevent the criminal use of the Internet by child sex offenders.
- ECPAT supports public education and awareness programmes which can reduce the risk to children of either becoming victims as the subjects of child pornography, or victims of seduction and exposure to harmful material through use of the Internet.
- ECPAT therefore also encourages the development of national hot lines and educational websites where children and adults can report child pornography and where they can learn about dangers from the use of the Internet.
- In its own operations ECPAT considers it inappropriate for its staff or members to be in possession of child pornography, unless this is done with specific permission of the local police and in co-operation with them, and in a strictly controlled environment for educational purposes.
- ECPAT does, however, encourage law-enforcement agencies to use demonstration examples of child pornography to selected audiences who have the potential to effect change in society, such as legislators or judges.

LEXICON

- **Browser:** a computer programme with a graphical user interface for displaying HTML files, used to navigate the World Wide Web
- **Chatroom:** an area on the Internet or other computer network where users can communicate, typically one dedicated to a particular topic
- **Download:** Copy data from one computer system to another or to a disk
- **E-mail:** the system of sending messages by electronic means from one computer user to one or more recipients via a network
- **Gigabyte:** a unit of information equal to one thousand million bytes
- **Internet:** an international information network linking computers, accessible to the public via modem links
- **Megabyte:** a unit of data size or network speed, equal to one million or 1,048,576 bytes
- **Login/on: Log/off/out:** go through the procedures to begin (or conclude) use of a computer system
- **Morphing:** change smoothly and gradually from one image to another using computer animation techniques or an image processed in this way
- **Newsgroup:** a group of Internet users who exchange email on a topic of mutual interest
- **Scanner:** a device that scans documents and converts them into digital data
- **Software:** Programmes and other operating information used by a computer
- **Upload:** transfer data to a larger computer system, the action or process of uploading
- **Usenet:** An Internet service consisting of thousands of newsgroups
- **Webpage:** a hypertext document accessible via the World Wide Web
- **Website:** a location connected to the Internet that maintains one or more web pages.
- **W.W.W. (World Wide Web):** an extensive information system on the Internet providing facilities for documents to be connected to other documents by hypertext links



- What are the new technologies and how do they work?
- What is an ISP and why are ISPs important?
- How do people communicate?
- What other common software do child exploiters use?
- Why do child exploiters like new technology?
- What is child pornography?
- Why is child pornography a key issue?
- What steps have been taken internationally?
- What are the major legal issues?
- What about freedom of expression?
- What can protect children on the Internet?
- How do filtering and rating software packages work?
- What is being done now?
- What can you do?