

### **A Challenge for the Real World**

*by Major Giorgio Stefano Manzi, Italian Internal Affairs Ministry, International Police Cooperation Department*

Global action to counter the commercial sexual exploitation of children cannot be exclusively repressive but should concentrate on preventive measures. In this respect, the study of possible current and future scenarios is important, particularly when it comes to technological advances and second-guessing the way they will be used by those who would harm children.

Child pornography, for example, involves the physical abuse of a child as well as the distorted use of technologies that are being perfected with the intention of benefiting the world. At the same time, the virtual 'non-places' where abusive and exploitative images of children are exchanged and where children are groomed for abuse are no longer only chatrooms, Internet Relay Chats (IRC) and newsgroups. Now, infancy as a commodity is consumed in new Internet spaces, such as those created by Multi-User Dimension (MUD) systems, through new resources for data transmission, and in the practice of sex tourism in countries still unable to combat this crime against children.

The evil use of new technologies is of particular concern as we act on the present and look to the future. I remember how, in the early 1990s, paedophile pornographers began to utilise newly emerging bulletin board systems (BBS) to exchange pornographic materials. These systems were territorially confined. The cost was affordable only if connections were made within the same telephone district, because connections were made by dialling into the Public Switched Telephone Network (PSTN) and transcontinental connections were still expensive. With the expansion of the Internet – and its affordability – the first mailing lists appeared, within which the first online 'communities' of paedophiles and other sexual abusers of young people developed. People on these restricted lists began to exchange not just textual messages but also pictures and movies. 'Old' technologies were still used, as photos were scanned for input and analogue films were made into newer digital formats. Soon, these paedophile mailing lists evolved into news groups (long-distance and geographically diverse, or telematic, discussion groups) in which anonymity favoured the extreme degeneration of both text and graphic production.

By the late 1990s, new technologies' unintended facilitation of anonymous networking and sharing of materials among paedophiles generated a pro-paedophilia 'ideological' boost and the spread of a paedophilic 'culture', whereby the likes of the Paedophile Liberation Front and NUMBLA used websites – often resident in countries with lax Internet and child protection laws – to promote adults' use of children for sex and tolerance of paraphilia, or dangerous sexual desires. Consequent to the development of techniques for encrypting online texts and graphics, such as through the use of steganography (see panel at left), more restricted paedophilic groups were created. Not only were audio-video-graphic materials (progressively more immediate because they were produced directly in a digital format) exchanged, but information was shared on the physical and actual availability of children, very often the sons and daughters of members of the groups.

The internal organisation of these groups, with names such as Shadows Brotherhood, Fun Club and The Group, reveals a tendency to esotericism and medieval corporatism. It is worth noting how an agreement to share materials through a kind of 'blood pact' has an economic character, and that at the core of these paedophile rings is a mutually binding 'contract'. Each member can then access the entire information patrimony of the group (that is, the children, data on how to find them, the material produced), while adding their own information as proof of loyalty. Bonding may also involve the exchange of information about how to approach criminal networks in countries affected by sex tourism, so as to arrange meetings with children in a 'protected' environment.

Analysed from the criminological point of view, the Internet has been transformed in recent years into a big store where paedophiles and voyeurs can look or shop around for 'articles'. They can go to websites for the provision of photos and films, to newsgroups for the sharing of mailing lists and URLs (the link to a particular Internet site), to IRCs in order to identify, groom and approach children, and to systems of instant messages. These are enhanced through encrypted plug-ins (software that adds extra features to these programs).

Too often, however, the 'technological' paedophile is confused with hackers or crackers, whereby the former is regarded as engaging in deviant behaviour from the informatic point of view. This is far from true. The paedophile exploits the technology, he controls it, but he does not abuse it. On the contrary, he is very attentive not to fall prey to the traps of software or copyright piracy. His presence is silent as he moves through the underbrush of encrypted systems of communication, in the virtual tunnelling systems, Secure Shells (see panel), in Voice Over IP (which allows phone calls over the Internet, so feared by police investigators). Arrogance is not his daily habit. He is a terribly 'serious' criminal. He is so serious that he meditates on the new borders and territory to be invaded: the Telnet, for example, (see panel) in order to modify the initially carefree and joyful nature of MUD. Or to exploit the third-generation mobile phone system, avoiding the Internet monitoring, in order to reach a child directly.

It is widely accepted that MUD systems (see panel) are among the newest challenges in efforts to counteract the abuse and exploitation of children, directly and indirectly, via the Internet. This is because the level of risk for a child is extremely high in the virtual non-places of MUD, where the related interactive games commonly attract teenagers. Adults who engage a child through MUD often aim to 'transform' the child's sexuality, by presenting him or her with different and sexually undefined identities. The ultimate goal in subjecting the child to 'dialectic tortures' is to confuse the young interlocutor about their gender identity, by means of continuous sexual solicitations, until the child enters a 'land' of marked perversion in which the abusive adult means to assume the role of guide. Evil and perverse.

A new scenario is rapidly coming true, along with what the (positive) theorists of the web have foretold for a long time. We are witnessing the transformation of a mere technological tool into a complex meta-instrument through which new realities can be created, realities that seem closer and more similar to the real world than can be imagined. The children of the world – our children – must be protected not only from exploitation, physical and worldly violence, but also from the dangers that loom within new communications systems. The dangers of physical and psychological harm emanating from the unreal but seductive spaces that paedophiles and other abusers of children infest – like a technological cancer – are being launched as yet another challenge to defenders of children. We will meet this challenge.

## **What does it all mean...**

### **Broadband**

A high-speed, high-capacity transmission channel for simultaneously passing multi-media information, such as pictures, videos and data between users.

### **Encryption**

A process by which data is converted into a format that may not be read or accessed by a human or a computer without the proper mechanisms to decode it.

### **Internet Relay Chat (IRC)**

A form of instant communication over the Internet (similar to instant messaging using MSN or Yahoo Messenger). It is mainly designed for group communication in discussion forums called channels, but it also allows one-to-one communication.

### **MUD**

Multi-User Dimensions is a computer program that allows multiple players to connect simultaneously through an Internet server to engage in a shared game or activity. Sometimes known as Multi-User Dungeons because the concept derives from the Dungeons and Dragons games, some MUD programs allow for 'social' contact (discussions etc) while others involve users in role-playing. A user can adopt and take control of a computerised persona or character in a 'fantasy' realm.

### **Secure Shell**

A program to log into a computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications.

### **Steganography**

The art and science of hiding messages within data for an intended user. On a webpage, for example, a steganographic message will appear to be something else, such as an article, a picture, or a 'cover' message.

### **Telnet**

A way to access a remote computer (with permission), as if you were logged on directly. This allows the user to call up any files or programs on the remote computer, and to issue commands as though they were sitting at it. Telnet can enhance the functioning of MUD systems.

### **Third-generation (3G) networks**

The next generation of wireless networks incorporating the use of mobile phone technology into a multi-media setting. It will allow users to keep connected to the Internet at all times and places, sharing a wide range of information in all formats and at immense speeds.

## **Europe leads way to address legal loopholes**

*by Karin Johansson, Programme Officer for Legal Matters, ECPAT Sweden*

The European Union (EU) clearly states that child pornography is increasing and spreading through the use of new technologies and the Internet. Now, it has taken an important step in seeking to criminalise some uses of the new technology, through the EU Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography, which entered into force in December 2003.

Legislators and law enforcement often have been one step behind people who deal with child pornography on the Internet. The Internet is a jungle that seems impossible to legislate completely. Due to the rapid evolution of new technology, perpetrators quickly change their methods when they recognise that law enforcement is closing in on them, and legislators and law enforcement all over the world have not been able to put an end to the increasing availability of child pornography on the Internet. With the EU's framework decision, however, law enforcement should be able to take more and harder actions against those who use and those who make and distribute child pornography, not only in the EU but also in other regions that follow Europe's lead.

The framework decision describes what actions regarding sexual exploitation of children and child pornography should be criminalised in each of the union's 25 member states. Under the decision, all acts including the production, distribution, dissemination or transmission, supply or making available, acquisition or possession of child pornography are to be criminalised, whether a computer system is used for any of this or not.

The decision makes it possible to prosecute anyone who contributes to this criminal activity in any way, thus taking a big step towards closing loopholes and ensuring that Internet-related child pornography use and distribution can be acted against more successfully, right across Europe.

A critically important element has been to include in the framework decision a definition of child pornography that refers not just to images of abuse of real children, but also to images of 'artificially created' children engaged in sexually explicit conduct. This means that images that are produced with computer animation are classified as child pornography, even where no real child is used to make the image. The definition also includes 'morphed' images, whereby pictures of real people are digitally altered, or several pictures are put together to look like one picture, for example, where an image of an adult is made to look like a child. This is a significant step forward because it shows recognition that all child pornography, whether it involves the exploitation and abuse of a real child or not, is a violation of the rights of all children and should be criminalised.

The EU member states have until 20 January 2006 to take the necessary legislative measures to comply with the framework decision. The laws in some countries may already be in accord with the framework decision, for example in criminalising people who buy access to child pornography. But several European countries will have to change their national legislation to comply with EU law.

Among these countries is Sweden, which as an initial measure has increased the maximum penalty for gross child pornography crimes from four to six years' imprisonment. By 'gross', the Swedish penal code means the production and wide distribution of child pornography, for which there is a heavier penalty than possession of such material. While the Swedish Government believes this is the only legislative change it needs to make to comply with the framework decision, ECPAT Sweden argues that at least one more change is necessary. This change has to do with the acquisition of child pornography, whether or not the material is downloaded.

Purchasing child pornography on the Internet with credit cards is a common procedure. In late May 2004, Swedish police carried out a coordinated raid, the biggest of its kind in Sweden, against 118 Swedish men who are all accused of buying access to child pornography on the Internet with their credit cards. The police are now examining the evidence and it will probably take months before anyone is brought to trial. No charges have been laid yet.

To be prosecuted for criminal possession of child pornography in Sweden, the accused has to be proved to have downloaded images, be they still photos or films, onto a hard drive, CD-ROM, DVD or a similar device. Accessing child pornography sites by buying entry with a credit card, for example, is not considered a criminal offence if the buyer has not saved the pictures onto his computer or printed them.

There have been several cases in Sweden where people have gone free because of this loophole in the national legislation. At least two of the men arrested in the May raid are making use of this loophole in their defence. It remains to be seen how many others among the 118 arrested will resort to a similar defence.

The EU Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography is a globally important first step to criminalise the myriad ways in which new technology such as the Internet is used for the purposes of sexually exploiting children, whether the abuser/exploiter harms a child directly in the making of pornography or further harms a child by accessing such materials. Hopefully, it will have a great input into national legislation in and outside the EU. And hopefully, one day, legislation and law enforcement will not be several steps behind criminals who sexually exploit children, but ahead of them.

### **Internet safety must be a priority**

*by John Carr, NCH Internet Adviser*

Around 1995-96, the Internet started its long march towards the mass market, away from the high-octane world of military research and big business and the more trusting cloisters of the academy. Everyone connected with children's education and welfare could see the Internet's potential benefits. But it was not long before the downside became apparent. The amount of child pornography being produced and circulated increased immediately. Chatrooms became a hunting ground for paedophiles. Pornography was everywhere. But when child protection agencies tried to talk to people in the British Internet industry about these things, with only one or two honourable exceptions, we were almost invariably met with hostility. This hostility derived from notions of free expression and an attitude that business was not responsible for content and how individuals used the Internet.

The notion that wider society, or democratically elected politicians, or their civil servants should have a say in anything to do with the Internet was anathema to those who felt it was their invention. But the initial rush of enthusiasm for the Internet meant that, in one sense, it did not matter how awful some of these start-up Internet companies were (in terms of how bad they were as businesses, their indifference to the wider social agenda, or their insufficient attention to thinking about some of their customers). New customers just kept on coming. But then three things began to happen.

The number of appalling cases involving online and related real-world sexual abuse and exploitation of children continued to rise. The Internet bubble burst, margins got tighter, and every net business had to look to its customer base in a different and more careful way. Thirdly, the number of Internet users was reaching a new critical mass, exposing Internet companies to new types of customers who were not geeks but 'ordinary people' with different attitudes and priorities.

Running alongside this were two further key developments. Initially, few civil servants understood anything about the Internet, and even fewer politicians. They did not want to interfere with it because of the economic growth it seemed to promise, and they did not know how to anyway. Self-regulation became the mantra, but it was a doctrine of expediency, not of choice. The same was true within law enforcement. In 1995-96, operational police personnel who actually knew about modems could be counted on the fingers of one hand. These conditions no longer apply, and many people within government and law enforcement now have a sophisticated grasp of Internet-based applications for communications and other new technology developments. Secondly, there have been important improvements in technology. Faster processors, cleverer artificial intelligence systems and the spread of broadband are perhaps the most important.

The first sign of a major shift in business attitudes towards recognition of their social responsibilities with regard to protecting children (against both harmful materials and people) was Microsoft's announcement last September that it was withdrawing from the chatroom market altogether, except in those countries (Canada, Japan and the United States) where MSN was established as a fee-paying service and where the company therefore had some data about who logged on. This decision has been both praised and treated with cynicism. But for my own part there is one irreducible and undeniable fact: I believe there is evidence that Microsoft will go some way to ensure its brand is not associated with, or even in the same space as, anything to do with child abuse and exploitation or any illegal sexual images. For example, Microsoft is funding much research and activity that seeks to address these and other related issues.

Next came two momentous decisions from Britain's mobile phone network operators, which are preparing for the introduction of third-generation (3G) networks linked to new and sophisticated handsets with Internet access. In January 2004, all six of them decided to introduce an age-verification system for all handsets connected to their networks. Unless you can show that you are 18 or above, from December 2004 your handset will not be able to access a range of adult content and services on the operators' own networks. Chatrooms have been

classified as an adult service, and one or more of the operators is likely to classify Internet access as an adult service. As well, anyone who wants to publish any material through the networks' channels will have to classify it as being suitable either for universal access or adult-only access. All six of the relevant 3G companies have also said they are pre-installing filtering and blocking software on all their network servers.

Now, British Telecom (BT) announced in June that it would block access to all known child pornography sites. Under the new system, a 404 error message appears when anyone types in, whether by accident or design, an address that has previously been identified by Britain's Internet Watch Foundation as containing abusive images of children. It is as if the page does not exist. Already, three other British-based Internet service providers (ISPs) say they will follow BT's lead, and children's organisations plan to press all the others (about 400) to follow suit. Inquiries to BT from overseas ISPs are also known to be flooding in.

BT's move to block illegal websites is a logical consolidation of a decision by all ISPs in Britain in 2002 to block access to all known newsgroups that contain child pornography. As a result, there were almost no reports last year of any illegal images on newsgroups across Britain. The inability to log onto such newsgroups from British-based ISPs has made a huge dent in the traffic, and made it impossible for most people in Britain to find such sites. Nonetheless, BT was brave to step forward and acknowledge that, technically, the blocking of websites containing child pornography could indeed be done, when other businesses were somewhere between hostile and very lukewarm to the idea. It has set the standard that others will now have to meet.

The way I see it, in Britain we have a happy confluence of four streams. The first is an energetic and effective NGO sector that is campaigning for progressive change in this area. The second is a more self-confident government and a law-enforcement community that now seems more willing to intervene on behalf of the wider public interest. The third is a new kind of business leader in the technology sector that is sensitive to these currents and wants to embrace and endorse them in a search for a larger market share. Finally, technological advances and cost reductions have underpinned all of the above and transformed the aspirational into the actual.

The challenge for all of us in the ECPAT network is to generalise these achievements and adapt them to our local conditions so we can make real inroads into the problem on a worldwide basis. These technical and policy fixes will never be enough on their own. They must work alongside first-class education and awareness programmes, but they are a very good start. At the end of the day, we need to assert that it is no longer appropriate, if it ever was, to think about the Internet as an adult medium, where special measures are needed to make provision for children's occasional or intermittent use. It is clear that children and young people are major and constant users of the Internet. If anything, they are disproportionately represented among Internet users. We need to start thinking about the Internet as if it were a main street or town square, not a night club. Website home pages should be thought of as public spaces, rather like shop windows. If we can gain acceptance for this idea, it has profound implications for global Internet policies and would mark the evolution of the Internet from wild frontier to civilization.

*NCH is a children's charity in Britain. John Carr is also a member of the British Home Office's Internet Taskforce on Child Protection.*

### **Credit cards: Room for action against criminals**

*by Dr Sarah Philipson, Telecom Consultant for ECPAT Sweden and formerly the Vice-President at TeliaInfoMedia*

Much of the child pornography distributed online involves no monetary exchange. Nevertheless, a lot is bought – often by using credit cards, which means it is technically possible to trace the transaction between the seller and the buyer. But so far, credit card companies have been unwilling to assist in such tracing, partly due to the web of intermediaries between them and the vendors. Tracing such transactions would not solve the problem of child pornography, but it would play an important part in countering its wider distribution, especially at the level of a buyer's first payment for such material.

When a peddler of child pornography recruits a new customer, they usually have to use an established commercially available payment system. The simplest ones are credit cards or billing services (invoicing services provided by telecom operators or utility companies). Credit cards give the vendor the money immediately and make it easy for the customer to complete the transaction. Credit cards also give the vendor the advantage of a global payment system, while billing services usually have to be based on local national service providers.

But once a customer becomes recurrent, the method of payment may be moved off the Internet. Arrangements may be made for buyers to make direct payments to special bank accounts, which are constantly changed to avoid detection. When the buyer-seller relationship enters into this phase, it is very difficult for the police to get to them, unless the crime ring is busted for other reasons and police get access to the vendor's billing records.

In light of this, the police may be best off to concentrate on finding crime rings as they recruit new customers. However, credit card companies and banks will need to provide much more support than they have done so far.

### **Hotlines a major force to combat child pornography**

*by Theo Noten, ECPAT Netherlands*

Hotlines are an important example of collaborative action against online child pornography as members of the public, Internet service providers (ISPs), hotline staff, local and international police work together against those who access and distribute child pornography over the Internet. One such hotline is Netherlands-based Meldpunt, which collects reports of online child pornography and refers information to the police. A rising percentage of complaints it receives result in charges being laid. Yet these reports also indicate that digital cameras, web-cams and scanners are facilitating easier distribution of child pornography while more aggressive tactics are being used to direct people to access such material.

In 2003, Meldpunt, which works closely with ECPAT Netherlands, received 5999 complaints, leading to 3914 reports registered with national police forces. In the Netherlands alone, Meldpunt reported to the police 208 incidents of child pornography distribution. Almost 100 cases went to court. The high number of reports leading to criminal charges in the Netherlands is a consequence of the close link between the hotline operators and the Dutch police, who trust the expertise of Meldpunt to assess whether the child pornography reported to the hotline is liable to prosecution. In cases requiring action abroad, and depending on the country in which the material originates, Meldpunt sends its reports to other hotlines associated with INHOPE (International Network of Hotlines Combating Illegal Material Online). INHOPE is a partnership between many European hotlines and others from around the world and coordinates hotline responses to illegal use and content on the net.

The number of complaints to Meldpunt last year was roughly the same as in 2002, but reports of child pornography rose by 67 per cent. This increase was mainly due to reports on spam (unsolicited email) referring people to websites containing child pornography, which in turn lead to websites offering even more disturbing material. These sites commonly have URLs originating in places with inadequate child pornography laws, such as the Commonwealth of Independent States (CIS). In its 2003 report, Meldpunt noted the deluge of spam suggested a growing commercialisation of child pornography, and more research was needed on this.

Another disturbing trend is that many reports, especially those concerning MSN groups and associated accounts, suggest that the images being circulated are extremely violent and depict more and more very young children. No money changes hands in these groups and membership is usually gained by sharing one's own images. In the case of reports concerning MSN groups, whose anonymous hotmail accounts all originate in the US, police outside the US must refer to American authorities all reports linked to MSN services, a process that slows counteractions.

Until law enforcement everywhere proves up to the task, hotlines remain critical to acting against online child pornography. But they are a tool and not a solution. Until all governments implement adequate laws and provide good support for their enforcement, URLs in lax countries will still be used to disseminate child pornography. We must continue to lobby for adequate legislation and law enforcement worldwide, and pressure the communications industry to act against commercial sexual exploitation of children. In the meantime, support must be provided to existing hotlines and for setting up new hotlines in countries where none exist.

For more information, see [www.meldpunt.org](http://www.meldpunt.org) and [www.inhope.org](http://www.inhope.org)

## **Planning ahead for the mobile generation**

*by Stuart Hyde, Assistant Chief Constable, Combating Child Abuse on the Internet, West Midlands Police*

Third-generation (3G) phones will put the world wide web in your pocket, making it even more accessible and deliverable. In Britain, the main licence holders for doing this have funded their new businesses to the tune of 20 billion-plus pounds. That's about US\$35 billion.

With 3G due to arrive in the mass domestic market in Britain soon, the impact of its introduction into Japan some three years ago is worth investigation. Earlier this year, I visited Japan with colleagues to see the likely consequences of this new technology and to assess the social implications. Our delegation met members of various political parties to debate issues that affect child welfare, including the impact of new technologies.

In December 2002, Vodafone KK launched its 3G network in Japan, where it is the country's seventh largest taxpayer. It bills customers on the volume of information that is uploaded or downloaded by the user and says that about half of the content downloaded has 'adult' themes. The company has raised concerns about children's safety vis a vis fast and easy access to the Internet via handsets, particularly with regard to dating sites, which have been linked to a rise in sexual and other violent crimes. While much of the social change around the use of dating sites in Japan occurred before the new technology became commercially available, the ubiquity of the Internet and increased capacity for the storage of data or images may be one factor linking the sites with crimes against children.

Mobile phone and online dating is a particular Japanese phenomenon that has grown from an older practice known as enjo kosai. Meaning 'compensated dating', enjo kosai can be a euphemism for what is, in effect, prostitution. This could include situations where an adult seeks a 'date' and sex with a child, in return for cash or gifts. In Japan, this practice used to centre mainly on telephone clubs. But the growth in 3G technologies means it has increased substantially through mobile phones and websites.

The crimes connected to these clubs range from murder and rape to extortion and prostitution of children. These types of crimes are known collectively as *teri-kura*, or telephone crime.

Japan's National Police Agency has responsibility for cyber crime committed within Japan and also plays a role in promoting security and safe Internet usage. According to the agency, reports of prostitution of children arising through the use of dating services via either mobile phones or personal computers increased by 95 per cent between 2000 and 2003. In the same period, there was a great increase in child pornography. At present, 20,000 legal dating sites exist in Japan.

In view of its concerns, Vodafone KK has developed a new range of mobile phones with standard security features that allow parents, guardians or carers to set 'limit modes' on their own or a child's phone. This effectively restricts access to certain sites or functions, unless the password is known. This has yet to be evaluated to judge its effectiveness, but it at least allows for some form of 'client-side' security. Controls discussed by Vodafone KK centre upon age verification prior to access, and parental controls that can be enabled on the user's device.

The full development of an age-verification system is likely to be a key tactic to protect children when they use handsets. More investigation on this issue is needed. But in Britain, Vodafone has at least taken a positive step in requiring that customers prove they are aged over 18 and provide credit card details before blocks on websites with adult content will be removed. Following on from British Telecom's action to block online child pornography, Vodafone is the first mobile company to take similarly oriented action to protect children.

The evolving situation in Japan raises many issues for consideration with regard to protecting children everywhere against the potential risks posed by 3G technology. Some of these issues include the following.

- In Britain and elsewhere, for example, 3G will increase connectivity and continue to blur the line between a simple telephone and Internet access.
- 3G technology allows an 'always on' functionality, and this has the potential to be exploited by criminals who want to remain mobile while uploading or downloading illegal content.
- It is essential that we strive to develop protective software and protocols before 3G is even introduced in other parts of the world.

- We also need to encourage the development of commercially available software that can be used to extract and reproduce information in an evidential format.

- The British and other publics need to learn about and understand what Internet safety programmes are being developed and introduced into schools, and complement this with action to ensure their children's protection at home.

We want the world wide web in the pocket to be safe. In view of the way young people will use this new technology, it probably needs to be made even more safe than the web accessed from a desk. Only by working together with industry and government will we achieve that.

## **Child Pornography and Online Solicitation**

Child pornography was identified by young people at the Second World Congress as a key issue concerning them. The ECPAT network has also identified it as an area of concern and much effort has been invested in developing solutions. As the theme paper prepared for the Congress pointed out, “child pornography is at once both a form of child abuse and also a representation of it” and “amplifies and broadcasts the original act of abuse”.

Max Taylor of the COPINE project notes that child pornography is “primarily domestic in character, with perpetrators having legitimate access to the child”. This may explain why research by the American Bar Association’s Center on Children and the Law indicated that children used in pornography are generally younger than those exploited in other ways.

New technologies have made image manipulation extremely easy, thus producing ‘virtual children’ and a genre of child pornography called pseudo-pornography. In the US, a child pornography Act which banned this form of pornography was regrettably struck down as unconstitutional in a recent legal challenge by the Free Speech Coalition.

The arrival of the Internet, and its popularity, has introduced a new problem: online solicitation of sex. In a TV spot aimed to raise awareness it is noted that the Internet has become the “hunting ground” for paedophiles. A survey carried out by the Crimes Against Children Research Center in 2000 revealed that one in five youth in the United States have been solicited for sex online.

Responses to child pornography on the Internet are varied. They include, but are not limited to, legislative measures, reporting hotlines, rating and/or filtering software, and the involvement of Internet Service Providers. Some individuals and voluntary associations have resorted to hacking into sites and closing down servers/pages that carry child pornography. EHAP in the US and Condemned in Australia are two such organisations, that are motivated largely by a moral stance against child pornography and a frustration with law enforcement or ISP related delays. Typically, responses to online solicitation of children focus on raising awareness among young people, teachers and guardians, and providing guidance to youth on “surfing” safely on the Net.

### **Victim Identification**

*by Max Taylor*

Child Pornography and the Internet – where should we focus our attention? This may seem a pointless question, because we all know the answer – the child victims of course. But without a complaint from a child, we need to identify the offender who can then lead us to the child. A unique feature of child pornography on the Internet, however, is that there may be evidence available from a photograph or from Internet data to aid that identification.

There have been dramatic successes where children have been identified in this way. But there are two points that need to be made to place this into context. One, despite enormous resources devoted to Internet child pornography by law enforcement agencies, few children are identified. It is impossible to get accurate data, but an estimate, based on material available to the COPINE Project, would indicate 40 to 50 children identified over the last 4 to 5 years, primarily in Europe and the U.S. Over that same time period, several hundred new children have appeared in child pornographic material – clearly it is a cause for concern that so few children are identified. Second, in terms of the incidence of child sexual abuse in general, the numbers appearing in child pornographic material on the Internet are low. No-one can estimate the number of children sexually abused over the past 4 or 5 years, but it clearly includes many thousands of children. What we see on the Internet is merely the tip of an enormous iceberg.

This presents an enormous challenge to the authorities. Internet child pornography is visible evidence of sexual abuse, and it both attracts a lot of public and political attention, and also offers opportunities for detection of offenders that non-Internet sexual abuse does not. In this lies the challenges for law enforcement and child protection agencies and Governments. As relatively few children are ever identified, should we place more resources into the identification of children? After all, a child pornographic picture is a picture of a sexual assault in progress. Or, should attention be directed towards disrupting collecting and trading activities involving child pornography? Where should the balance lie?

Many people are arrested for possession of child pornography, but highly publicized cases can give a false sense of what is being achieved in terms of child protection. Reasons for this are a tendency to equate possession of child pornography with the commission of contact offences, and a failure to distinguish between different kinds of offences involving child pornography. Most offenders who download child pornography do not have any relationship with the child portrayed. Operations that disrupt and hopefully diminish the amount of trading in child pornography do not substitute for the identification of the children involved.

However, the identification of child victims is difficult, and it is much easier for the Police to focus on offenders involved in collecting rather than producing child pornography. Evidence suggests that there are different kinds of offenders involved with child pornography, some of whom are involved in contact offences (through the production of material) but others who are not, and collect rather than produce material. High profile police actions directed at the collectors may aspire to reduce the availability of child pornography, although given the nature of the Internet that is unlikely. They can also serve as deterrents for other collectors; but they generally contribute little to the identification and protection of the children who have been photographed.

A commonsense approach suggests that policy in relation to child pornography should have two agendas – the primary agenda must relate to the protection children where possible who are being sexually exploited. Police organizations are central to this, as the investigative arm of multidisciplinary teams, who are trained in the forensic and computer skills necessary to effectively pursue investigation. The secondary agenda should relate to the disruption of child pornography trading networks, making collecting and possession of child pornography, and/or facilitating its access the subject of effective deterrents, through the judicial process. Reducing the demand for child pornography through making possession an increasingly risky and dangerous activity is a worthwhile contribution to child protection. However, the principal agents in this latter activity must be Internet Service Providers. Police action and effective government regulatory activity will enable this to occur.

However, it must be stressed that there is little point in developing strategies for the identification of victims, if the necessary support structures are not available, or sufficiently developed. An alarming trend in new child pornography is a growing number of pictures that appear to come from disadvantaged communities in either Eastern Europe or South America. Both policing and social welfare infrastructures in these locations are often very poor, and it is likely that no matter what processes of identification are brought to bear, the unfortunate victim in these circumstances is unlikely to receive much by way of support and therapy.

Where a focus on victims can be developed, it will involve close interagency liaison (i.e. between the investigating police officers and the social welfare or therapeutic teams dealing with the child). This implies a much greater degree of commonality of approach and a sharing of information than is often currently the case.

Above all however the needs of the child involved must remain paramount, and social welfare or law enforcement agencies should have as their primary objective the empowerment of victims, however administratively or politically inconvenient that might be.

*Max. Taylor, is Professor and Head of Department of Applied Psychology, at University College Cork, Ireland. He is also Director of the COPINE Project, which is developing a victim identification project with Radda Barnen and Childnet (<http://copine.ucc.ie>).*

## **Pseudo Pornography and Freedom of Speech**

*by John Carr*

In the US and in several other jurisdictions, historically the justification for banning child pornography was that its production necessarily involved an actual child being criminally abused.

However, modern computers and software can artificially create entire pictures which present a child pornographic image that is indistinguishable from a depiction of a real event. Alternatively, computers can take a picture of a wholly innocent event and change it into something completely different and obscene, or parts of an innocent image can be grafted on to an existing indecent image to create a new image. The new picture may contain edited parts of a real child's body, or even the full representation of a whole child, but either way the event depicted never actually happened. This is what is now known as pseudo-pornography and in most countries no distinction is made between it and actual child pornography.

In 1996 the US tried to join this happy band of nations when it passed the Child Pornography Prevention Act. However Congress did not reckon with the so-called Free Speech Coalition, an “adult trade association”, who challenged the legality of the Act. The case has just been heard by the US Supreme Court. On a 6-3 majority and, sadly, the Free Speech Coalition seem to have won. However, the Justices expressly did not rule out the possibility that a more narrowly drawn law might succeed in the future.

One of the more disingenuous points the Coalition advanced was that they were worried that if Congress could make laws in this area it would inevitably lead American society down the “slippery slope of suppression”. You always know you have won the argument when the other side trots out the slippery slope. It is another way of saying “OK you are right about this, and we know it, but if you obtain the change you are seeking it will inevitably lead to other things, which will probably also be right, but which we do not want because they will cost us money or harm our business interests.” In other words it is egregiously immoral.

A full report of the case is still not available but observers were hoping that the Justices would take the opportunity to clarify several grey areas of the law. For one thing, where any part of the body of a particular child has been used to create an image in such a way as to allow anyone to identify the child in question, the image cannot truly be called “pseudo”. For that child it will be very real and, amongst many other things, almost certainly a violation of their right to privacy. And what if the image of the child is wholly artificial but one or more real adults involved?

Civilized society has declared, or ought to, that any image which purports or seeks to show children being sexually abused is undesirable and unacceptable in principle. This is not just because of the harm it does to any children who may be its actual or immediate victims. By its very nature child pornography also has wider consequences and a broader impact that cannot be overlooked. Viewing child pornography can desensitise adults and lead them towards further harmful or abusive behaviour, and therefore puts other children at risk. In a study carried out by the US Postal Inspection Service it was established that over 35% of those arrested initially for mere possession of child pornography were also contemporaneously engaged in sexually abusing children.

As Sir William Utting (People Like Us, HMSO, 1996) and others have noted, child pornography can be highly instrumental in nature, desensitising or sexualising children in inappropriate ways. Child pornography is used by sexual predators quite deliberately to lure children into abusive relationships. They try to prove with pictures that sex between an adult and a child is normal and fun. In that context, therefore, whether or not the image is real or artificial is of absolutely no significance. If it looks like child pornography it should be treated as if it were child pornography.

Seeking to make, essentially theological differences between different types of equally realistic images, is irrelevant in the real world. Does anyone imagine, anyway, that the producers of pseudo-pornography will faithfully emblazon all their work with a health warning saying “All the characters in this image are completely artificial. Any resemblance between them and real persons is completely unintended.” No! The very point of doing it is to represent real events. And imagine the absurdity of arrested child pornographers arguing that every image is artificial and then it is for the prosecution to show that the images are in fact real. Will the prosecution have to produce the actual children in court and get them to testify as to the genuineness of the events depicted and their part in them? Are children to be forced to relive the trauma of the original abuse?

The great bulk of child pornography today is found on the Internet. Huge numbers of children are very frequent visitors to cyberspace. Thus, perhaps for the first time ever, children themselves are at risk of being exposed to child pornography on a substantial scale. What is the Free Speech Coalition proposing to say to them? That, actually, they believe images of children having sex are OK, providing only that it can be established the persons depicted are not real? And just how are they proposing to ensure that the children know the persons are not real? Truly this is a case where we should judge the book by looking only at its cover?

Societies frequently have to balance the rights of private individuals against wider societal interests and we should all instinctively be wary of allowing the state greater powers in relation to what individuals may or may not do. So what this case comes down to is a question of priorities. Is it more important for the state to protect the right of someone to view certain forms of child pornography than it is to protect children from the harm that those images could cause? To ECPAT members and supporters the answer is obvious. Seemingly it wasn't to the US Supreme Court Justices.

*John Carr is Associate Director of the Children & Technology Unit at NCH, one of the UK's leading children's charities (www.nch.org.uk). He is also a member of the UK Government's Task Force on Child Safety on the Internet and is Internet Adviser to the UK's Children's Charities Coalition on Internet Safety.*

### **Hotlines and staff welfare**

*By Theo Noten and Linda Venselaar*

Since the Dutch hotline Meldpunt was established in 1996 the amount of reports received by the hotline have steadily increased. In 2001, the hotline received almost 5000 emails containing one or more reports about possible illegal content. Staff check and classify these reports by assessing whether the material meets the criteria of article 240b Sr of the Dutch Penal code.

Thus, the staff of the hotline are exposed to hundreds of images and videos, including very serious child pornography where there is clear evidence of physical force. Each day, they witness many cases of sexual abuse of a child, and although this abuse might stop, the proof of it will stay forever and is distributed all over the world.

Quote of hotline staff member: "For four years now I am doing this job and there have been lots of moments that I sat crying before my computer screen. Although it comforted me to think that I contribute to the combat of the distribution of child pornography, it still is a scary thought that some of these images might stay with me the rest of my life. What will happen to these thoughts when I quit my job. What will happen with these children?"

There are all kinds of reasons that hotline work can get to you and in the end the only thing one can do is to stop. To prevent this and to take up their responsibility to take care of the welfare of their staff, Meldpunt explored the possibilities for psychotherapeutic counselling. After having consulted the police on how they handle this, Meldpunt decided to work with a psychotherapist, specialised in treating victims of sexual abuse and sexual exploitation and specialised in counselling programs to prevent post traumatic stress syndrome. Now all hotline staff who are exposed to child pornography images have regular structured sessions with the psychotherapist.

Staff welfare is becoming a highly important area for all Hotlines. The danger of post traumatic stress caused by exposure to particular images has been clearly recognized and has been raised as an issue of concern at various INHOPE (Association of European Hotlines) meetings. The psychotherapist working for Meldpunt has also joined one of the INHOPE meetings to give a workshop about the prevention of secondary traumatizing.

The need for early recognition of problems in members of the staff and the availability of incident debriefing in the event of exceptional trauma has to be well structured and thought through. Counseling is a necessary tool in taking care of hotline staff members' welfare and contributes to the hotline's continuity.

*Theo Noten is campaign manager for ECPAT-Netherlands. He is participating in the project team for the implementation of the Dutch National Action Plan. He is member of the board of the Dutch hotline Meldpunt Kinderporno. Linda Venselaar is staff member of Meldpunt Kinderporno and is participating as their representative in INHOPE meetings.*