Journal of Information, Law & Technology

Online Child Safety from Sexual Abuse in India

Lina Acca Mathew
Cochin University of Science and Technology, Kerala State, India
linamathew@yahoo.com

This is a **commentary** published on 28 May 2009.

Citation: Mathew, Lina A., 'Online Child Safety from Sexual Abuse in India', 2009(1) *Journal of Information, Law & Technology (JILT)*, <http://go.warwick.ac.uk/jilt/2009_1/mathew>

Abstract

Abusing children with the aid of information and communication technologies is becoming a world-wide problem. In the context of the Mumbai terror attack in November 2008, wherein terrorists used internet, mobile and satellite technology in communication, an urgent need for enacting laws for controlling new-media crimes was felt in India. The existing Information Technology Act of India, 2000 contains a general provision in section 67 which punishes the publishing of information which is obscene in electronic form. The Information Technology Amendment Act 2008 was passed by the Indian Parliament in December 2008 and received Presidential assent in February 2009. A final notification remains for its entry into force. The Amendment Act includes a new section 67B wherein electronically depicting children in sexually explicit acts, as well as abusing children online has been made an offence and punishment prescribed accordingly. A new subsection 2 (ha) also extends the term 'computer network' to include 'communication device' which includes cell phones. Despite these progressive steps taken to protect children online, considerable limitations still remain. This paper suggests a definition of the offence of 'Online Child Sexual Abuse'. It examines initiatives taken by the US, UK, EU and other international agencies against sexual abuse of children through the internet. and tries to strengthen the law in India relating to online child sexual abuse. A multi-layer approach of governance comprising of techniques for promotion of child safety measures, prevention of the offence and protection of the child is seen as essential for India to combat online child sexual abuse and developing a civil society which is pro-active to the needs of children.

Keywords

Online sexual grooming-inadvertent/accidental access- online child sex abuse images/child pornography- online child sexual abuse- The Information Technology Amendment Act of India, 2008-Offences against the Child (Prevention) Bill of India, 2007

1. Introduction

The World Health Organization defines child sexual abuse as the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or that violates the laws or social taboos of society. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person. This may include but is not limited to the inducement or coercion of a child to engage in any unlawful activity, the exploitative use of a child in prostitution or other unlawful sexual practices, the exploitative use of children in pornographic performances and materials[1]. A similar definition has been stated in Article 18 of The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse, 2007 which is yet to enter into force[2].

The risks that minors face online include sexual solicitation, exposure to problematic and illegal content as well as harassment and bullying. These risks are not confined to their local area but

occur from people all around the world. Parents and teachers do not have direct experience with the risks posed by new-media technologies. Addressing the risks online therefore carries different challenges and requires broader collaboration to find innovative solutions[3]. The need for a multi-layered approach to internet governance in India is highlighted by a comparative study of the various measures available internationally to make communications over the information and communication technologies safe.

A concerted effort is very essential from various actors in order to prevent online child sexual abuse. Those who can help report child sexual abuse have been identified as social-service workers, healthcare practitioners, education providers, law enforcement officers, photo developers, IT professionals, ISPs, credit card companies and banks[4]. Other actors are telecom service providers, network service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes. A multi-level sensitisation about the need to collect statistics as well as report suspected internet child abuse should be effected among these actors.

In India, the government does not take a pro-active stand against child sexual abuse, in contrast to the USA where law enforcement officials lure potential sex offenders in decoy. In sting operations conducted in the USA, where paedophiles are lured over the internet to contact people below the age of consent over the Internet for sexual liaisons, many highly-educated and well-to-do Indians are turning up as potential molesters. This is particularly disturbing, as there are no statistics on this in India[5].

Child-to-child solicitation and abuse through the medium of mobile telecommunications is becoming a serious problem in India. Other kinds of abuse occur through social networking sites like Orkut where pictures of girls have been posted on communities with lewd allusions and a listing of the victims' mobile numbers. With new-media technologies available at lower costs, child sex abuse images are being increasingly made and uploaded from India[6]. In a recent case in Kerala State, three girls committed suicide after increasing blackmail that the film of classmates raping them which had been taken on a mobile camera would be publicly circulated. Generally, it is a fact that unwanted publicity and fear of victimisation by law enforcement machinery are reasons why the largely conventional Indian families fear reporting child sexual abuse.

2. A Comparative analysis regarding definition and criminalisation of Online Child Sexual Abuse

The word 'online' means all forms of information and communication technologies like the internet, mobile phones etc. Three types of abuse of sexual nature that occur against children online are identified to be solicitation, providing access to sexually explicit content by minors and exploitation of children for child pornography. In the US, given the various standards applying to 'obscene' and 'indecent' pornography as well as 'material harmful to minors', the use of the word 'pornography' with regard to a child is fraught with difficulty. As pointed out by the Virtual Global Taskforce[7], the use of the words 'child pornography' legitimises child sexual abuse by relegating it to mere pornography. Hence a better term in this regard would be 'child sex abuse images'. This paper brings the three kinds of online sexual abuse and exploitation of child by all those in a position of responsibility, trust, or power under the umbrella of 'Online

Child Sexual Abuse'[8]. This paper suggests that the term 'Online Child Sexual Abuse' should include the following:

(1) Online sexual grooming of minors, which means enticing and soliciting the child for further offline abuse.
(2) Access to sexually- explicit content by minors, which means the child accessing obscene and harmful content including child sex abuse images, both intentionally and otherwise.
(3) Production or reception of online child sex abuse images, which means producing or receiving any online sexually abusive representation of a child. Here, 'child' means a person under eighteen years of age and would include both real as well as virtual children, as well as adults who appear to be children.

This section deals with an examination of the initiatives taken by the US, UK, EU and other trans-national agencies in combating the three types of online sexual abuse of children, outlined above, in comparison to India.

2.1 Online Sexual Grooming of minors

This includes online enticement as well as distributing or showing pornography (adult or child) to a child for further offline abuse, encompassing both child-to-child grooming as well as adult-to-child grooming. In the United States, the Protection of Children from Sexual Predators Act of 1998 makes it a crime to knowingly make a communication for commercial purposes harmful to minors or to use the Internet for purposes of engaging in sexual activities with minors or transmit information about a person below the age of 18 for the purpose of enticing, offering, encouraging or soliciting any person. The Broadband Data Improvement Act Title II deals with the Protecting Children in the 21st Century Act passed in 2008, required schools and libraries that receive E-rate funding to have an Internet Safety Policy which must include 'educating minors about appropriate online behaviour, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.' The 2008 Internet Safety Technical Taskforce (ISTTF) report on 'Enhancing Child Safety and Online Technologies found that youth report sexual solicitation of minors by minors over the internet more frequently, but these were understudied and underreported to the law enforcement. It was noted in the Literature Review by the Research Advisory Board[9] that there is an overlap between online harassment and solicitation of minors among child-to-child abuse.

In the UK, the Sexual Offences Act 2003 of England and Wales as well as the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 created an offence of meeting a child following sexual grooming. It is an offence to arrange a meeting with a child, for oneself or someone else, with the intent of sexually abusing the child. Under the Scotland Act, befriending a child on the internet or otherwise, and meeting or intending to meet the child with the intention to abuse him/her is made an offence. Thus, a crime may be committed even without the actual meeting taking place and without the child being involved in the meeting (e.g. if a police officer has taken over the contact and pretends to be that child).

Under these Acts, a new civil preventative order, the 'Risk of Sexual Harm Order' (RSHO), may be imposed which will prohibit adults from engaging in inappropriate behaviour such as sexual

conversations with children online. The four categories of behaviour that can trigger a RHO are engaging in sexual activity involving or in the presence of a child; causing a child to watch a person engaging in sexual activity - including still or moving images; giving a child anything that relates to sexual activity; and communicating with a child where any part of the communication is sexual. Any knowledge of such activity must be reported to the police right away. The Sexual Offences Prevention Order (SOPO) is another preventive order placed on a person who has been convicted of crimes with a sexual/violent element.

In the EU, the European Commission pledged US$377,600 to create a pan-European alert platform run by Europol where people can report illegal material on Web sites. The aim is for a platform to help investigators of online crime in E.U. countries to share information about all cyber crime, especially child porn, as child pornography accounts for over half of all offences committed online[10].

The Virtual Global Taskforce (VGT) aims to prevent and deter child sex abusers from committing online child abuse by working with online providers to make it more difficult for such abusers to misuse the Internet and by increasing the likelihood that those who go online to commit child abuse will actually be caught. It has conducted various sting operations on groomers that have solicited children online, and has got paedophiles convicted for online sexual abuse[11].

The Information Technology Amendment Act of India, 2008 (ITAA) makes it an offence under section 67B[12] to facilitate abusing children online. However, the term 'facilitates abusing children online' is not explained. The concept of online sexual predators grooming children is not specified in the Act. The rest of the sub-clauses outlines child pornography, cultivating, and enticing inducing child-to-child relationship for sexually explicit acts. An RSHO and SOPO in the lines of UK legislation, linking the Indian police with the VGT and Europol, raising awareness programmes in all youth meeting points regarding issues like online solicitation, stalking, harassment and bullying by adults-to-minors and minors-to-minors are measures can be thought of to counter the offence of online sexual grooming in India.

2.2. Access to sexually- explicit content by minors

Intentional and unintentional exposure of children to sexually explicit content[13], including child sex abuse images, may have negative psychological or behavioural effects on children. Unintentional exposure may occur by accident or inadvertence in the form of pop-ups or misleading domain names, during otherwise innocuous activities. In the US, the restriction of children from pornographic sites is lined with controversy, because only 'obscene' pornographic sites in the US are considered as illegal, hence not protected by the First Amendment right to free speech. A definition of 'obscenity' was given in the landmark case *Miller v. California*[14], whereby only hardcore sexually explicit material could be classified as obscene and unprotected. Pornographic sites which are merely 'indecent' and not 'obscene' would be protected by the First Amendment. In order to circumvent this for the protection of children against pornography, the US Congress in 2003 made 'material harmful to children' to be illegal. A material is 'harmful' to a minor if it contains nudity, sex or excretion that primarily appeals to the prurient interest of the minor, is patently offensive to the prevailing norms as to what is suitable for a

minor and lacks serious literary, artistic, political or scientific value for minors. Thus, now in the US, material indecent for adults could come under the category of 'material harmful to children' and hence illegal for the child to access.

In the context of the Internet, the US government was unwilling to grant free speech exemptions to indecent speech harmful to minors, and sought in a series of legislations, to ban obscene speech over internet communications as well as speech harmful to minors. The Communications and Decency Act of 1996(CDA) criminalizes the knowing transport of obscene and indecent material for sale or distribution either in foreign or interstate commerce or through the use of an interactive computer service to minors. The U.S. Supreme Court struck down sections criminalizing the sending of indecent material to minors as unconstitutional under the First Amendment[15]. The Child Online Protection Act of 1998(COPA) covering only commercial communications and only material harmful to children was held as unconstitutional[16]. The Children's Internet Protection Act of 2000 (CIPA) regulates computer access to adult-oriented websites in public schools and libraries by installing filtering technology that prevents adults and minors from accessing material deemed harmful. The Supreme Court upheld the law as constitutional as a condition imposed on institutions in exchange for government funding, which applied only to minors[17].

In the US, the Prosecutorial Remedies and Other Tools to Tend Exploitation of Children Today (PROTECT) Act 2003, was launched to prevent sexual exploitation and other abuses of children. §2252B regulates the use of Misleading Domain Names which deceive a person into viewing obscene material or a minor into viewing material harmful to minors. A person who knowingly uses such a misleading domain name will be fined and/or imprisoned for not more than two years if the viewer is a person and/or imprisoned for not more than 4 years if the viewer is a minor. The Section characterizes a domain name as not misleading if it contains wording indicating the sexual content of the site. As such, a domain name indicating words such as 'sex' or 'porn' is not misleading. Thus, the Legislature succeeded in broadening the definition of 'material harmful to minors' to the same standard of obscenity laid down by *Miller*.

The 2008 ISTTF report identified three core concerns with respect to problematic content: (1) youth are unwittingly exposed to unwanted problematic content during otherwise innocuous activities; (2) minors are able to seek out and access content to which they are forbidden, either by parents or law; (3) the intentional or unintentional exposure to content may have negative psychological or behavioural effects on children[18]. Filtering and monitoring devices were found to be the most mature technological method. However, these technologies can be easily bypassed by those older minors who actively seek out such inappropriate content[19].

In the UK, in 1996, a national hotline called the Internet Watch Foundation (IWF) was launched, undertaking to inform all British ISPs once undesirable content is located. The UK police will be entitled to take action against any ISP which does not remove the relevant content requested from IWF. Rating systems like PICS[20], content filtering at source for child pornography like CleanFeed are some devices used in UK for regulating content.

Within the European Union also there have been developments with regard to protection of minors against illegal content. In October 1996, the European Commission launched a

Communication Paper on Illegal and Harmful Content along with a Green Paper on the 'Protection of Minors and Human Dignity in Audio Visual and Information Services'. Following this the European Parliament adopted a Resolution in April 1997. From 1999 to 2004, the EU launched the Safer Internet Action Plan and from 2005-2008 Safer Internet Plus programme aimed at creating a safer environment through the promotion of hotlines, encouragement of self regulation and codes of conduct, developing filtering and rating systems, facilitating international agreements on rating systems and awareness amongst parents, teachers and children. Yet another initiative partly funded by the European Commission is INHOPE, which facilitates and coordinates the work of 23 national hotlines against illegal Internet content, as well as coordinates and exchanges information and expertise between hotlines worldwide. Thus the European Commission has adopted a system of self regulation by ISPs themselves.

Cyber-zoning is the division of the cyber space into various zones, for example, the kids-only zone, adults-only mature zone etc. It has been suggested as a remedy to need for constant monitoring of what children are watching on the Net[21]. By blocking all other zones other than the kids-only zone, parents can safely leave their kids with the Internet. The Dot Kids Implementation and Efficiency Act, 2003 launched the heavily regulated .kids.us sub-domain, which lists prohibited contents, including mature content, inappropriate language, drugs, violence, tobacco, gambling, weapons and criminal activity. Currently only the US has a .kids.us sub-domain.

In 2005, there was a proposal to create a .kid Top Level Domain (TLD) for the EU, as well as a proposal for the ICANN to create a for-profit .xxx TLD for adult websites and a non-profit .kids TLD as an integrated solution for improving child safety on the Internet. It was an attempt to implicitly restrict content across both TLDs in order to protect children from exposure to online pornography as well as to have a positive impact on online adult entertainment through voluntary efforts. These were abandoned. The reason for less popularity of cyber-zoning is the difficulty in regulating pornographic content, as the definition of pornography varies by jurisdiction. Also, creation of a .xxx TLD would result in the legitimisation of pornography[22].

A legal provision specifically addressing the issue of distributing obscene material to minors in India is section 293 of the Indian Penal Code, 1860 (IPC), which punishes the sale, letting on hire, distribution, exhibition or circulation of obscene material to any person under the age of twenty years. Here the offer and attempt are penalized[23]. Accessing sexually explicit material online would not come under the ambit of section 67 of the Information Technology Act 2000 which punishes the 'publishing', 'transmitting' and 'causing to be published' obscene material in electronic form, which are not explained. Since 'access' is just the opposite of 'transmit', such access of sexually explicit material cannot be punished under section 67 of the IT Act, or under the new provision 67A [24] of the ITAA 2008. Taking a cue from the US, an additional offence of facilitation of accidental/inadvertent access by a child to sexually explicit material through misleading domain names and pop-ups containing sexually explicit material could be made under the ITA in India.

Various state-level hotlines are being contemplated under the aegis of the Computer Emergency Response Team of India (CERT-In), which has been given statutory status under ITAA as the national nodal agency to look into matters containing cyber security. A problem that is

particularly troubling in India today is that there are various instances of children capturing their sexual dalliances with other children over mobile cameras and transmitting these files to their friends. Such hotlines should have close contact with all telecom providers regarding undesirable content being accessed by children.

2.3. Production or reception of online child sex abuse images

This indicates producing or receiving any online representation, of a child engaged in real or simulated sexually explicit activities or any representation of the sexual parts of the child for primary sexual purposes, as well as engaging in the use of the child to create such representation. This shall include:

i. Online access to files containing images of abuse (both real and simulated) committed on children including custom child sex abuse images where sale is of images of child sex abuse created to order for the consumer
ii. Online access to real time images of children being sexually abused (through real time technologies like the web cam).

Article 34 of the United Nations Convention on the Rights of the Child 1989 (UNCRC) lays down that all signatories shall take appropriate measures to prevent the exploitative use of children in pornographic performances and materials. The subsequent Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography mandated international obligations to pass specific laws against child pornography 'punishable by appropriate penalties that take into account their grave nature' as well as enable extradition, mutual assistance in investigation, and seizure of property. The Optional Protocol further stated that member states of the United Nations were 'concerned about the growing availability of child pornography on the Internet and other evolving technologies…' Thus, child pornography over the internet came within the ambit of the UNCRC.

Three primary reasons to be concerned about online child pornography are (1) offenders who view and trade child pornography create a demand; (2) deviant sexual fantasies based on Internet images may fuel a need to sexually abuse other children; (3) child pornography is sometimes created during the grooming process by both solicitors and youth victims (which may or may not be initiated online)[25]. However, the use of the terminology 'child pornography' is not to be encouraged[26]. Hence this paper uses the terminology 'online child sex abuse images'.

In the US, federal regulation called the Child Pornography Prevention Act of 1996 (CPPA) was enacted, wherein §2256 prohibits and criminalizes the use of computer technology to knowingly produce child pornography that contains both depictions of real children as well as 'virtual' or fictitious children. Provisions against virtual child pornography in the CPPA were ruled unconstitutional by the U.S. Supreme Court[27] on the grounds that the restrictions on speech were not justified by a compelling government interest (such as protecting real children). The PROTECT Act 2003 penalizes transport, producing, receiving, distributing of visual depictions of sexually explicit conduct by minors. Section 2252A(a)(3)(B) prohibits offers to provide or requests to obtain obscene material depicting actual or virtual children engaged in specified sexually explicit conduct, and any material depicting actual children engaged in sexually explicit

conduct. This section was struck down as unconstitutional, being overbroad and vague. In May 2008, the U.S. Supreme Court[28] upheld the constitutionality of this Act. Thus virtual children are also prohibited from being depicted in obscene material in the USA.

The U.K. Obscene Publications Act 1959 places tight controls over printed pornographic material[29]. The Criminal Justice and Public Order Act 1994 made electronically transmitted obscene data to be covered by the 1959 Obscene Publications Act. This made the ISPs liable for content even though in some circumstances they did not consent to the publication of the material. With regard to child sex abuse images, in the UK, the Protection of Children Act 1978 (as amended by the 1994 Act) makes it an offence to take, make, permit to be taken; distribute or show; or possess with a view to their being distributed or shown (by the defendant or others) any indecent photograph or indecent pseudo-photograph of a child. As of the commencement of the Criminal Justice and Immigration Act 2008, this prohibition will be extended to encompass 'tracings' of photographs. In 2008, the Government announced its further plans to criminalize all non-realistic sexual images depicting under-18s. Thus in the UK, virtual child sex abuse images is being prohibited. In 2007, under pressure by the British Government, ISPs have decided to block pages containing online child abuse material which are listed in the IWF database. But this approach only prevents accidental viewing of such sites. Content delivery over encrypted connections, email, instant messaging, or seemingly innocent P2P sites cannot be regulated in this way.

The first International Treaty, the Convention on Cyber Crimes dealing with computer based criminal offences was entered into force in 2004 by members of the European Union. Child pornography is defined here as pornographic material that visually depicts a minor, a person appearing to be a minor or realistic image representing a minor engaged in sexually explicit conduct.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse (Child Protection Convention), 2007 broadens the Cyber Crimes Convention's definition of child pornography to include both real and simulated images of sexually explicit conduct as well as depiction of a child's sexual organs for primarily sexual purposes. It has not yet entered into force. From 2006-2007, Child Exploitation and Online Protection Centre (CEOPC), the UK agency of VGT, led an international operation into a UK-based paedophile ring in 2007 smashed a global online child abuse network and rescued 31 children from abuse or positions of harm. Two British nationals were convicted in English courts for making, possessing and distributing indecent images and movies of children.

The 2005 ECPAT (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes) study on 'Violence Against Children in Cyberspace' detailed studies of children from Mexico, Nepal, the Czech Republic, the Philippines, India and Moldova, all of whom had been implicated in a range of sexually abusive activities including production of child pornography. This was the first study that documented that all children, not only those who had access, were potentially vulnerable to harm through the new technologies.

In November 2008, the World Congress III against the Sexual Exploitation of Children and Adolescents in its Rio de Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and

Adolescents[30] called on States, UN agencies, NGOs, the private sector, academia, children and young people and other relevant actors to press for development of voluntary Codes of Conduct and other corporate social responsibility mechanisms as well as provide incentives to the private sector for research and development of robust technologies to identify images taken with electronic digital cameras and trace and retract them to help apprehend the perpetrators. Countries are to commit to working more closely with Interpol on a child abuse imagery database and establish a special children's desk for crimes against children. It called for an abolition of double criminality (where perpetrators cannot be tried unless there are relevant laws in both their home country and the country where the crime was committed) in cases of sexual exploitation of children.

The 2008 ICMEC (International Centre for Missing and Exploited Children) study 'Child Pornography: Model Legislation and Global Review' analyzing 187 Interpol countries concluded that only 29 have legislation sufficient to combat child pornography offences and 93 countries have no legislation at all that specifically addresses child pornography. The five criteria used in the test were: whether national legislation: (1) exists with specific regard to child pornography; (2) provides a definition of child pornography; (3) criminalizes computer-facilitated offences; (4) criminalizes possession of child pornography, regardless of the intent to distribute; and (5) requires Internet Service Providers (ISPs) to report suspected child pornography to law enforcement or to some other mandated agency. According to this study, mere criminalization of child pornography alone is not enough. It recommended that the definition of child pornography should include computer and Internet specific terminology; criminal penalties should be ensured for parents or legal guardians who acquiesce to their child's participation in child pornography; grooming offences be criminalised; mandatory reporting to be necessitated; criminal liability of children involved in pornography be addressed- that children are only victims and criminal liability must focus on the adult offender; sentencing provisions to take into account aggravating factors and enhancements; assets be forfeited and proceeds used to support child victims etc.
Going into the Indian situation, the 2008 ICMEC report points out that India satisfies three criteria of the five – namely, national legislation exists specific to child pornography, national legislation exists specific to computer-facilitated offences and national legislation exists criminalising simple possession of child pornography, regardless of the intent to distribute. Accordingly, no national legislation in India defines child pornography, nor is there any national legislation which mandates ISP reporting.
In India, it can be seen that, on a national level[31], the offence of child pornography could only be read into section 292 of the IPC which is a general prohibition on possession of obscene material, as well as section 293 which prohibits the sale of such obscene material to minors. Sections 292-294 of the IPC punish offences relating to obscene material[32]. Hence there was no national legislation specific to the offence of child pornography, nor was the offence defined at the time the ICMEC Report was published in 2008. The existing Information Technology Act of India, 2000 contains section 67 which is a general provision which punishes the publishing of information which is obscene in electronic form. The ITAA having received Presidential assent in February 2009, a final notification of entry into force remains for it to become an offence to electronically transmit material depicting children in sexually explicit acts and facilitating online child abuse, under section 67B. Thus, we shall have a national legislation defining acts which would constitute the offence of online child pornography. But there is no national legislation specific to the general offence of child pornography.

Under section 292 IPC, both possession and making available obscene material is punished[33]. Distribution of such obscene materials to minors is made punishable under section 293. In this way, possession of child sex abuse images is punishable under a general provision of national legislation. Even though the word 'possession' of online child sexual abuse material is not used per se, however, 'collecting' of such material is punished under sub clause (b) of section 67B, hence the criterion of the 2008 ICMEC study shall be complied with.

Regarding criminalization of computer-facilitated offences, under section 67 of the Information Technology Act 2000 (ITA), based on section 292, it is an offence to publish and transmit obscene information in electronic form[34]. Thus publishing and transmission of child sex abuse images would come under the ambit of this section. However, section 67B of the ITAA can deal more specifically with the offence[35]. A difficulty here is that the term child is not defined. It is recommended that the word 'child' is to be explained as real and virtual children as well an adults appearing to be children.

A highlight of the ITAA is to enlarge the scope of definition of 'computer network' so as to include 'communication device' which means 'cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image' (Sec. 2(ha) of the ITAA). As a result of this, the ITAA has been made applicable to online child abuse material available through mobile networks.

In February 2008, it was reported that the GSMA, the global association for mobile firms, launched the Mobile Alliance[36], which plans to create significant barriers to the misuse of mobile networks and services for hosting, accessing, or profiting from child sexual abuse content. The members of the Alliance commit to implement 'Notice and Take Down' procedures that will enable the swift removal of any child sexual abuse content which they are notified about on their own services. In Sri Lanka, the National Child Protection Authority of Sri Lanka and Dialog GSM announced in October 2008 the signing of a Memorandum of Understanding (MoU) to restrict access to websites which carry child sexual abuse content through mobile phones. Such agreements with Indian telecom service providers could be made part of governmental policy.

2.4. A comparison of laws regarding mandatory reporting

The ICMEC, in its 2008 Report, recommended mandatory reporting by various individuals and organizations of suspected child pornography activities and offences to law enforcement or another specified agency[37]. In the US, a 1996 federal law called the Electronic Communication Transactional Records Act (Title 42) regulates data preservation. It requires Internet providers to retain any record in their possession for 90 days 'upon the request of a governmental entity'. Also, internet providers are required to report any child pornography sightings to the Cyber Tip Line at the National Centre for Missing and Exploited Children, which is in turn charged with the duty of forwarding that report to the appropriate police authority. The 2008 ICMEC study recommending model legislation on child pornography included the US as one among five countries which comply with all the five identified standards.

In the UK, despite the functioning of the Internet Watch Foundation (IWF), which reports undesirable content to British ISPs for removal of undesirable content as mentioned in sub-

section 2.2, there is also no statutory provision in the UK for mandatory reporting of the ISPs of material relating to online child sexual abuse. As a result, the 2008 ICMEC study shows the UK having only 4 of the 5 stipulated statutory provisions to curb child pornography.

In India, under the ITA 2000, network service providers are made not liable for third party information or data made available by them as long as it is proved that they have no knowledge or exercised due diligence to prevent the offence (section 79). However, the Computer Emergency Response Team of India (CERT-In) can block websites which have no constitutional right to free speech (like online child sexual abuse images) without prior notice. With the advent of the ITAA 2008, the intermediaries[38] will have to keep detailed accounts of the information handled by them for a specified period. Intentional contravention of the requirement pertaining to preservation and retention of data will entail imprisonment up to three years and fine. The CERT-In or other Government-authorised agency shall monitor content over computer networks including mobile communications[39]. If offending content is found, it shall inform the intermediary to disable or remove such offending content. If the intermediary does not do so, liability accrues. If service providers, intermediaries, data centres, body corporate, or any other person fail to provide the information called for or comply with such direction, the punishment provided is imprisonment up to one year or with fine up to one lakh rupees or both. This model of intermediary liability is based on the UK practice. To make intermediary liability more in tune with the ICMEC 2008 recommendations, such intermediaries could be compelled to mandatorily report to an agency authorised by the government. Such mandatory reporting of offences against children was contemplated in the former draft Bill Offences Against the Child (Prevention) Bill 2007[40]**.** Mandatory reporting by personnel of studios or photographic facilities, stakeholders providing accommodation facilities as well as those providing transportation facilities, is made compulsory. However, the drafters were sceptical about the workability of mandatory reporting in India, given the long delays of around 20 years for disposal of rape cases. But, I submit that if such an attitude were to be taken, this would result in under-reporting of child abuse and the perpetuation of the crimes by the offender because no one wants to let the police know fearing further victimisation by the law enforcement system. Instead of discouraging mandatory reporting, the better way would be to make policy that will dispose cases in speedy and humane way.

2.5. India—an analysis of section 67B

Section 67B in the ITAA shall make it an offence to publish or transmit material depicting children in sexually explicit acts in electronic form, and facilitating online child abuse[41]. In section 67B, ‘child sex abuse images’ or ‘child pornography’ as it generally referred as, is not defined specifically. The act of making available electronic child pornography can be inferred from a combined reading of clauses (a) and (b). The term ‘sexually-explicit’ has not been defined. As pointed out in sub-section 2.3, the term ‘child’ has not been explained in the context of online children. What would constitute ‘abuse’ under clause (d) has not been specified. Regarding this, one meaning of abuse can be the offence of online sexual enticement and solicitation for offline abuse. Another kind of abuse could involve the real time transmission of images of children being sexually abused through technologies like the webcam. As pointed out earlier, the collection of ‘sexually-explicit’ images of a child in electronic form is made an offence under clause (b) of section 67B, as recommended by the ICMEC study in 2008.

The status of the online child under the ITAA has not been clarified. The 2008 ICMEC study specifies that the child involved in pornography is a victim, and should be treated regardless of whether he/she is a compliant victim or a non-cooperative witness. Both under the Immoral Trafficking Prevention Act and the Indian Penal Code, sexual exploitation of a child under 16 years of age in India is statutory rape (consent is immaterial), so the law should be interpreted to treat children under 16 years of age as victims in need of care and protection. Unless the child is treated as a victim and given compassionate treatment by law enforcement authorities, it is doubtful whether parents will be willing to report online abuse to the authorities for fear of further victimization by the criminal justice system. On the other hand, it should be stressed that child offenders who actively abuse other children have to compulsorily be subject to the rehabilitative and reformative treatment measures provided for in the Juvenile Justice (Care and Protection of Children) Act, 2006. Section 82, IPC, exempts all acts done by children below the age of seven years from criminal liability. Section 83 states that nothing is an offence which is done by a child above seven years of age and under twelve, who has not attained sufficient maturity of understanding to judge of the nature and consequences of his conduct on that occasion. Hence it would be necessary to read into the ITAA those provisions in the Indian Penal Code regarding the acts done by a child.

The ITAA empowers police officers from the rank of Inspector upwards to investigate, enter and search public places without a warrant for evidence so as to facilitate speedy delivery of justice. The Indian police force has been equipped by the establishment of cyber police stations in various states to combat cyber crime. However, there is no mention in the ITAA of a national cyber police wing to assist the CERT-In and to coordinate the state cyber police cells. As per international recommendations, abetment and attempt crimes are made punishable (sections 84B and 84C). The ITAA has given due importance to the seriousness of electronic crimes against children, by attributing punishment that makes the offence under section 67B cognisable and non-bailable[42]. As per the proviso in section 77A, the Court shall not compound any offence where imprisonment exceeds three years. So an offence under section 67B is non-compoundable, too. Yet another safeguard that can be made applicable to child sexual abuse content is the section 66E of the ITAA which criminalises the intentional or knowing capture, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, in circumstances where a person can have a reasonable expectation that (*i*) he or she could disrobe in privacy, without being concerned that an image of his private area is being captured; or (*ii*) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place. This protection of privacy is very relevant in cases of child sexual abuse images that are increasingly being captured on mobile cameras.

3. Child safety legislations and child online sexual abuse in India

Would the grievances of the child victim regarding online child sexual abuse be better redressed by procedure under the Information Technology Act or under a separate legislation dealing exclusively with child safety laws? In India, child sexual abuse cases take an inordinately long time to get decided, and various measures may be taken by the offenders in order to circumvent conviction, the net result being further victimisation of the child victims by the law enforcement system. Pointers are the *Swiss Nationals*' as well as the *Anchorage* cases, which are still

unresolved[43]. The Goa Children's Act of 2003 (amended in 2005) pioneered as a comprehensive law on child protection laying down child-friendly practices in tune with the UNCRC to be followed by the State of Goa and its courts. Under the section criminalising 'child abuse', punishment is meted out for sexual assault, grave sexual assault and incest. Soliciting children for purposes of commercial exploitation is prohibited, which includes hosting websites, taking suggestive or obscene photographs etc. The term 'commercial sexual exploitation of children' means 'all forms of sexual exploitation of a child including visual depiction of a child engaged in explicit sexual conduct, real or stimulated, or the lewd exhibition of genitals intended for sexual gratification of the user, done with a commercial purpose, whether for money or kind.' The definition of 'grave sexual assault' was expanded by the 2005 amendment to include acts like making children pose for pornographic photos and films, forcing minors to have sex with each other, deliberately causing injury to sexual organs of children, etc. Developers of photographs or films, as well as Airport authorities, border police, railway police, traffic police have to report sexual/obscene depictions of children, suspected cases of trafficking of children etc. The preparation of a Child Code by the Goa Police including Child Friendly Police Stations, prohibition of children below 14 years arriving unaccompanied inside any cyber café, constitution of a Children's Court- adopting child-friendly procedure like age of innocence, principle of best interest, principle of non-stigmatizing semantics, etc are envisaged. However, the Children's Courts have acquitted many cases of paedophilic abuse citing insufficiency of evidence.

The national legislation Commissions For Protection Of Child Rights Act 2005 envisages constitution of children's courts in a state or districts for the purpose of providing speedy trial of offences against children or of violation of child rights. As per this Act, in March 2007, a National Commission for Protection of Child Rights (NCPCR) in India was set up. Another development was the draft Bill titled Offences Against the Child (Prevention) Bill 2007 proposed by the Ministry of Women and Child Development, which was rejected by the Law Ministry. This draft Bill attempted to incorporate international recommendations on child rights. As in the Goa Act, 'child-friendly' principles and procedures were enunciated. The principle of non-criminalization of a child at all stages of the proceedings is laid down. Sexual assault, when committed by a public servant, staff or management of a Children's Institution, school staff etc. comes under the category of 'grave sexual assault'. But unlike the Goa Children's Act, making children pose for pornographic photos and films was not included under 'grave sexual assault'. Showing pornography to a child was classified as a 'non-contact based sexual offences' which is based upon having an intention to achieve sexual gratification. Instead of using the word 'grooming', the offence stated was 'act(s) undertaken with intent that such person could at any point of time in the future, sexually assault a child or undertake any form of unlawful sexual contact'. Also, 'commercial sexual exploitation' does not include a new-media facilitated commercial exploitation, as in the Goa Act.

Among offences relating to pornography, electronic representation of the sexual organs of a child or children, usage of children engaged in real or stimulated sexual acts (with or without penetration) and the representation of a child in any indecent manner, for sexual gratification, such media including programmes and advertisements, telecast by Television channels, irrespective of whether it is intended for personal use or for distribution, shall be guilty of the offence of pornography. Possession of child pornography and knowledge of child pornography

cause liability for imprisonment that may extend to seven years or fine or both. This provision in the draft Bill would address the lack of specific provision in Indian law for punishment for possession of child sex abuse images. The draft Bill provided for giving medical care and counselling to a child within 24 hours through establishment of Child Trauma and Counselling Centre in every District Hospital and shall comprise of an Emergency Response Team. In all cases, non institutional methods would be preferred, along with rehabilitation services including sustained counselling and institutionalization shall only be adopted as the last resort, when it is in the best interest of the child or will prevent the child from being re-victimized. Various protective and preventive measures including creation of a well trained work force, constitution of community-based child-offence-prevention, Vigilance Committees at the National, State and District Level, Research and data-base creation regarding Child Rights and Child Protection, making obligatory facilitation of a 'Personal Safety Education' by all schools to empower a child, conducting such discussions with the parents and the teachers were mandated.

Regarding Children's courts to be constituted under Section 25 of The Commissions for Protection of Child Rights Act, 2005, detailed provisions were given regarding *in camera* judicial proceedings, protection of identity of the child victim and punishment of fine for disclosure of identity if any of the aforesaid acts is committed by any form of media-- the fine shall be the total revenue of that media, throughout the territory of India, for a complete day. There was a provision for legal aid to be given for a child or their families. As mentioned in sub-section 2.4, the issue of mandatory reporting was considered. This draft Bill did not address the issue of child-to-child abuse, where the offender is a child. The principle of abolition of double criminality, and promotion of extradition measures with regard to child sex offenders, also finds no mention in this draft Bill. Given the fact that a national legislation on child protection is not even a distant reality, what can be done in the near future is that courts dealing with offences under section 67B should adopt a child-friendly procedure, effectively enforce the rights of the child victims as well as render speedy justice.

4. Conclusion

This study comes to the conclusion that there is no one-stop solution to the problem of how to protect child online. The new ITAA is just a starter in the combat against online child sexual abuse. A multi-layer approach of governance would be the need of the hour. The various techniques of promotion, prevention, and protection must be staged at local, regional and national nodes in order to make an impact upon the safety of the online child.

The government as well as educational institutions must evolve a comprehensive child safety policy in India at the grass root level, with emphasis on online child safety measures. Awareness programmes targeting teachers, parents and other caregivers, as well as local self governmental bodies, camps for children educating them how to keep safe online should be promoted as part of governmental policy. Parental control through filter technology and spy ware may be promoted as a mature solution to protect children from online sexual abuse. Responsible sexual attitudes must be urgently promoted in society, in keeping with the child's development, dignity, self esteem. Another tool to be considered is child participation. Promotion and monitoring of online safety on the curriculum in schools, youth organizations and at other meeting points for children is highly necessary. Establishing and supporting networks of children and young people as

advocates of child rights, and include children, according to their evolving capacity, in developing and implementing government and other programmes concerning them at the local, regional and national levels will go a long way towards empowering children through individual participation.

There is an urgent need for collection of statistics in India regarding the risks that minors face through new-media technologies. The 2008 ISTTF Report highlighting these as sexual solicitation, exposure to problematic and illegal content as well as harassment and bullying should be kept in mind. The effects of exposure to new-media risks should be scientifically studied and measures to counter such risks evolved. One pointer in this regard is the Indian Government entering into agreements with Indian telecom providers restricting access to websites which carry child sexual abuse content through mobile phones. Strong messages should be sent out by the government regarding strict penalties to accrue for employment of new-media technologies for sexual solicitation, harassment, distribution of obscene material to minors, as well as possession and distribution of child sex abuse images. This will definitely make young people more aware of the risks posed by new evolving technologies.

Regarding online child safety legislation, there should be definition of the various kinds of child abuse and exploitation occurring through information and communication technologies. A definition of child pornography should include all kinds of information and communication technologies. This paper suggests that 'Online Child Sexual Abuse' may be made an offence in India, and may include the following:

(1) Online sexual grooming of minors which is defined as online enticement as well as distributing or showing pornography (adult or child) to a child for further offline abuse, encompassing both child-to-child grooming as well as adult-to-child grooming.
(2) Access to sexually-explicit content by minors which is defined as the intentional and unintentional exposure of children to sexually explicit content, including child sex abuse images, through misleading domain names and pop-ups or other means during otherwise innocuous activities.

*Explanation***:** 'sexually explicit content' means actual or simulated --1. sexual intercourse, which includes genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; 2. bestiality 3. masturbation 4. sadistic or masochistic abuse; or 5. lascivious exhibition of the genitals or pubic area of any person

(3)Production or reception of online child sex abuse images which is defined as producing or receiving any online representation, of a minor engaged in real or simulated sexually explicit activities or any representation of the sexual parts of the minor for primary sexual purposes, as well as engaging in the use of the minor to create such representation. This shall include

iii. Online access to files containing images of abuse (both real and simulated) committed on minors including custom child sex abuse images where sale is of images of child sex abuse created to order for the consumer
iv. Online access to real time images of minors being sexually abused (through real time technologies like the web cam).

*Explanation***:** For the purpose of this section, 'child' or 'minor' means any person under 18 years of age and includes both real and virtual children, as well as adults who appear to be under 18 years of age.

Mandatory reporting by social-service workers, healthcare practitioners, education imparters, law enforcement officers, photo developers, IT professionals, ISPs, credit card companies and banks, telecom service providers, network service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes should be made a legal obligation. Children below 14 years should be prohibited from arriving unaccompanied inside any cyber café. A RSHO and a SOPO in the lines of UK legislation would considerably ensure child safety in general, and online child safety in particular, because of a distinct feature of the Internet, namely, anonymity. Criminal penalties should ensue upon parents, legal guardians, teachers, public officers and employees and all those in a position of trust to a child, who acquiesce and abet to the child's participation in such child sexual abuse. Punishments should be prescribed according to the type and gravity of the offence. As pointed out by the 2008 ICMEC study, aggravating factors may include the number of images manufactured/produced/distributed/possessed; the severity of the offender's existing criminal record; the sexual violence toward children (including rape, torture, and bondage) being depicted in the images that were manufactured/produced/distributed/possessed; and any potential threat or risk the offender may pose to the community upon release.

Child-friendly police stations and courts, ensuring speedy delivery of justice and the best interests of the child, must be the norm. Indian police cyber cells should coordinate with agencies like the VGT and Europol and join the combat against online child sexual abuse. Extradition measures and other arrangements should be promoted so that the person who exploits another child in the destination country should be prosecuted either in the country of origin or in the destination country. An abolition of double criminality in cases of sexual exploitation of children should be voiced internationally. In order to reintegrate the child into society, provision should be made for forfeiture of property, proceeds or assets that result from activities related to child sexual abuse. These funds should be used to support programs for formerly abused children, children at risk of being abused, and child victims who are in need of special care. A pro-active stand against societal stigmatization of child victims and their children would facilitate the recovery and reintegration of child victims in communities and families. Socio-medical and psychological measures to create behavioural changes in perpetrators of child sexual abuse should be taken. In cases of online sexual solicitation, child actively seeking out problematic content online, production of child pornography by child-to-child abuse, harassment/bullying/stalking leading to the offence of online child sexual abuse etc, where a child is actually the perpetrator, the age and stage of mental development of the child will have to be taken into consideration in determining the gravity of the offence, and the provisions of the Juvenile Justice Act, 2006 may have to be made applicable accordingly.

Thus, India must gear up to the challenge of adopting child-sensitive practices to protect the citizens of tomorrow and develop a responsible democracy.

References:

Akdeniz, Y. (1997), 'Governance of Pornography and Child Pornography on the Global Internet: A Multilayered Approach' in Edwards, L. and Waelde, C. (eds), Law and the Internet: Regulating Cyberspace (UK: Hart Publishing), <http://www.cyberrights.org/reports/governan.htm>

'Doesn't Every Child Count? Research on Prevalence & Dynamics of Child Sexual Abuse Among School Going Children in Chennai', <http://www.tulir.org/images/pdf/Research%20Report1.pdf>

ECPAT (2006), 'Global Monitoring Report on the status of action against sexual exploitation of children: India' , <http://www.ecpat.net/A4A_2005/PDF/South_Asia/Global_Monitoring_Report-INDIA.pdf>

ECPAT International (2005), 'Violence Against Children in Cyberspace' A contribution to the UN Study on Violence Against Children', <http://www.ecpat.net/EI/Publications/ICT/Cyberspace_ENG.pdf>

Final Report of the Internet Safety Technical Taskforce (2008), 'Enhancing Child Safety and Online Technologies', < http://cyber.law.harvard.edu/pubrelease/isttf/ >

Information Technology Act 2000 and the proposed amendments <http://www.naavi.org/naavi_comments_itaa/compare_2000-6-8/compare_2000-2008/index.htm>

International Centre for Missing and Exploited Children (2008), 'Child Pornography: Model Legislation and Global Review' 5th Edition, < http://www.icmec.com/en_X1/English__5th_Edition_.pdf>

Ministry of Women and Child Development, Government of India (2007), 'A Study on Child Abuse: India 2007', <http://wcd.nic.in/childabuse.pdf >

Online Child Safety and the Virtual Global Taskforce <http://www.ycwa.org/features/vgt.htm>

Sheldon, K. and Howitt, D. (2007), Sex Offenders and the Internet (UK: Wiley).

Smith, G. J. (2007), Internet Law and Regulation (London: Sweet and Maxwell).

Taylor, M and Quayle, E. (2003), Child Pornography—An Internet Crime (UK: Brunner-Routledge).

Weekes, R. B. (2003) 'Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access To Sexually Explicit Content on the Internet?', 8 Va. J.L. & Tech. 4 < http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf >

Wolak, J., Finkelhor, D. and Mitchell, K.J. (2005), 'Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study 2005', <http://www.missingkids.com/en_US/publications/NC144.pdf>

Wolak, J., Finkelhor, D. and Mitchell, K. J. (2005), 'The Varieties of Child Porn Production' in Quayle, E. & Taylor, M. (eds.) Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims (UK: Russell House Publishing), pp. 31–48

World Congress III against the Sexual Exploitation of Children and Adolescents at Brazil The Rio de Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and Adolescents, November 25-28, 2008
<http://www.iiicongressomundial.net/congresso/arquivos/rod_28_nov_final_ingles.doc>

<www.childsexualabuseinindia.blogspot.com>

---

[1] 'Ministry of Women and Child Development, Government of India (2007) 'A Study on Child Abuse: India 2007' at p. 73 <http://wcd.nic.in/childabuse.pdf>

[2] Article 18 states that 1. Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:
a) engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities; b) engaging in sexual activities with a child where:
– use is made of coercion, force or threats; or
– abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or
– abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.
For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.

[3] Final Report of the Internet Safety Technical Taskforce 'Enhancing Child Safety and Online Technologies' (2008) < http://cyber.law.harvard.edu/pubrelease/isttf/ >

[4] International Centre for Missing and Exploited Children (2008), 'Child Pornography: Model Legislation and Global Review' 5th Edition at p. 4 <
http://www.icmec.com/en_X1/English__5th_Edition_.pdf>

[5] 'Seven Indians held in sex sting operation in California' October 18, 2006 17:38 IST <http://in.rediff.com/news/2006/oct/18sting.htm>

[6] See 'CBI nabs man trading child pornography on Internet' 5th November 2007 <http://www.exbii.com/showthread.php?t=202026 >

[7] This is a joint initiative started in 2003 among certain law enforcement agencies around the world working together to fight online child abuse, by empowering children by raising awareness of the risks that children and young people face online as well as by providing tools to help manage those risks. See Online Child Safety and the Virtual Global Taskforce <http://www.ycwa.org/features/vgt.htm>

[8] Child abuse is defined under § 5106g (2) of 42 U.S.C.A as "Any recent act or failure to act on the part of a parent or caretaker, which results in death, serious physical or emotional harm,

sexual abuse, or exploitation, or an act or failure to act which presents an imminent risk of serious harm" Sexual exploitation includes allowing the child to engage in prostitution or in the production of child pornography.

[9] Schrock, A. and Boyd, D (2008), 'Online Threats to Youth: Solicitation, Harassment, and Problematic Content' at p. 28 < http://cyber.law.harvard.edu/research/isttf>

[10]'EU cracks down on Internet porn' October 24, 2008 <http://www.itworld.com/internet/56689/eu-cracks-down-internet-child-porn>

[11] *Supra*, n.7

[12] 'Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or (d) facilitates abusing children online; or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section do not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or (ii) which is kept or used for bonafide heritage or religious purposes. Explanation.- For the purposes of this section "children" means a person who has not completed the age of 18 years.'

[13] Here 'sexually explicit content' can be defined on the lines of § 2256 of the PROTECT Act 2003 of USA as: 'actual or simulated --1. sexual intercourse, which includes genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; 2. bestiality 3. masturbation 4. sadistic or masochistic abuse; or 5. lascivious exhibition of the genitals or pubic area of any person'

[14] 413 U.S. 15 (1973)

[15] Reno v. ACLU 521 U.S. 844 (1997)

[16] ACLU v. Mukasey (No. 07-2539) decided by 3rd Circuit Court of Appeals on July 22, 2008

[17] US v. American Library Association 539 U.S. 194 (2003)

[18] *Supra*, n. 10 at p. 29

[19] Final Report of the Internet Safety Technical Taskforce (2008), 'Enhancing Child Safety and Online Technologies' at p. 33<http://cyber.law.harvard.edu/pubrelease/isttf/ >

[20] The IWF recommends the use of rating systems such as Platform For Internet Content Selections (PICS), which is a rating system for Internet developed by the WWW.Consortium (W3C), a non-profit making association of academics, public interest groups and computer companies, that looks at the social consequences of technology. The PICS works by embedding electronic labels in the text or image documents to vet their content before the computer displays them or passes them onto another computer. A similar scheme is the RSACi, developed in the

United States by the Recreation Software Advisory Council for the Internet, which rates materials according to the degree of sex, violence, nudity and bad language depicted. Another rating system, called Safesurf, along with RSACi, uses the PICS format, but rely on Web sites to rate their own pages, while they reserve the right to verify each site's rating. Only a minority of existing Web sites is currently rated by these systems. Filtering software companies can add additional blocked sites to their databases on an ongoing basis. The various filtering software products offer a wide range of features including two way screening. Examples are Cyber Patrol, CYBERsitter, Net Nanny, Specs for Kids as cited in Appendix F Internet Filtering Software FTC <http://www.ftc.gov/reports/privacy/APPENDIXf.shtm#N_2_>

[21] Weekes, RB (2003), 'Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access To Sexually Explicit Content on the Internet?' 8 Va. J.L. & Tech. 4 < http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf >

[22] <http://en.wikipedia.org/wiki/.kids>, <http://en.wikipedia.org/wiki/.xxx>

[23] Punishment awarded on first conviction is 5 years imprisonment and fine up to Rs. 1 lakh. On subsequent conviction, imprisonment may extend to10 years and fine up to Rs. 2 lakh.

[24] Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

[25] *Supra*, n.10 at p. 37

[26] The Virtual Global Taskforce (VGT) states that such a phrase actually works to the advantage of child sex abusers in that the term indicates legitimacy and compliance on the part of the victim and therefore legality on the part of the abuser; conjures up images of children posing in 'provocative' positions, rather than suffering horrific abuse; and every photograph captures an actual situation where a child has been abused, which is not pornography. The November 25-28, 2008 summit in Rio de Janeiro, Brazil, of the World Congress III against the Sexual Exploitation of Children and Adolescents, noted in The Rio de Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and Adolescents: **"**Increasingly the term 'child abuse images' is being used to refer to the sexual exploitation of children and adolescents in pornography. This is to reflect the seriousness of the phenomenon and to emphasize that pornographic images of children are in fact records of a crime being committed."

[27] Ashcroft v. Free Speech Coalition 535 U.S. 234 (2002)

[28] United States v. Williams (No. 06-694) decided on May 18, 2008.

[29] Sec. 2 of the Act provided the following ingredients for obscenity"….an Article shall be deemed to be obscene if its effect is, taken as a whole, such as to tend to deprave and corrupt persons, who are likely, having regard to all relevant circumstances, to read, see, or hear the matter contained in it".

[30] The World Congresses against the Sexual Exploitation of Children are co-sponsored by the government of the host country, the UNICEF, ECPAT and the NGO group for the Convention on the Rights of the Child. The first World Congress took place in Stockholm, Sweden in 1996, the second in Yokohama, Japan in 2001. The World Congress III against the Sexual Exploitation of Children and Adolescents took place in Rio, Brazil in 2008.

[31] Except the state of Goa which has a Goa's Children's Act, 2003 amended in 2005 wherein the offence of child pornography is specifically laid down

[32] In order to be obscene, the material should be lascivious or appeal to the prurient interest; or its effect or where it is more than one item, the effect on any one of the items, if taken as a whole, is such as to tend to deprave and corrupt persons who are likely, having regard to all the relevant circumstances to read, see or hear it (section 292, IPC).

[33] Punishment on first conviction is imprisonment of either description for a term which may extend to two years, with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

[34] The punishments included imprisonment description up to a term of five years, and fine which may extend to one lakh rupees, and for subsequent conviction with imprisonment up to ten years and fine up to two lakh rupees. Under the Information Technology (Amendment) Act, 2008,(ITAA) the punishments have been altered so that first conviction incurs imprisonment up to three years and fine up to five lakh rupees, and subsequent conviction incurs imprisonment up to five years and fine up to ten lakh rupees.

[35] S*upra*, n. 13

[36] The Alliance has been founded by the GSMA, Hutchison 3G Europe, mobilkom austria, Orange FT Group, Telecom Italia, Telefonica/02, Telenor Group, TeliaSonera, T-Mobile Group, Vodafone Group and dotMobi.
See < http://news.bbc.co.uk/2/hi/technology/7238739.stm>

[37] *Supra*, n. 4

[38] The term 'network service provider' has been substituted with 'intermediary', to include telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes (section 2(w)).

[39]The definition in section 2(j) of the IT Act 2000 pertaining to 'computer network' has been widened by section 2(ha) of the ITAA 2008 to include 'communication device' which means 'cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image'. As a result of this, the IT Act has been made applicable to online child abuse material available through mobile networks.

[40] The Ministry of Women and Development proposed this draft bill so as to bring India on par with the UNCRC. However, the Law Ministry rejected it, saying that it was only a repetition of provisions in other laws. See <http://www.crin.org/violence/search/closeup.asp?infoID=14752>

[41] S*upra*, n. 13

[42] Punishment under section 67B is imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees. As per section 77B of the ITAA, offences punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of up to three years shall be bailable. Hence the offence under section 67B shall be cognizable and non-bailable.

[43] In 2003, two Swiss nationals Wilhelm and Lile Marti were convicted by a Sessions court in Mumbai for filming a pornographic video with two street girls in 2001. In 2004, the Bombay High Court granted bail after a deposit of six lakh rupees. The Supreme Court granted bail to

them, and asked them not to leave the country. However, in 2004 itself, they escaped the country with their passports still in the custody of the Sessions court. In the Anchorage case, Childline India Foundation received a call in 2001 on its helpline about child sexual abuse in Anchorage shelters. In 2006, a Sessions Court in Mumbai convicted two British nationals Duncan Grant and Alan Waters and their Indian accomplice William D'Souza for sexually abusing boys in the Anchorage shelter homes run by them in the State of Maharashtra. The British nationals were sentenced to six years rigorous imprisonment and 20,000 pounds fine, while the Indian was sentenced to three years. In appeal, the Bombay High Court in 2008 acquitted them citing insufficiency of evidence. The Supreme Court stayed the High Court judgement in 2008, and directed the police not to hand over the passports of Grant and Waters. They remain in India. The case is presently before the Supreme Court.