INDIAN JOURNAL OF HUMAN RIGHTS AND THE LAW | VOLUME 12 • NUMBER 1 JANUARY-JUNE 2015 • PP. 43-59

INADEQUACY OF LAWS PROTECTING CHILDREN AGAINST ONLINE SEXUAL ABUSE IN INDIA

KARNIKA SETH* AND RAMA SHARMA**

Abstract: Internet is not just a unique virtual space where one communicates with another or as a medium of entertainment or a rich source of information. Today Information Technology is a way of life not just for adults but also kids as young as 4 or 5 years. With several attractions through multimedia in form of educational videos, e books, nursery rhymes to online gaming and social media there is plenty on Internet to engage a child's attention. What rings an alert is the volume of uncensored content and content unfit for children that freely floats the internet and to add to one's fear is prevalence of organized racket operators, child groomers and cybercriminals that purposely target gullible children to victimize them and/or lure them into heinous crimes such as child pornography, sexual harassment, cyber-bullying and other related offences. According to a study conducted by Ministry of Women and Child Welfare in India in 2007, wherein over 12, 000 children were studied for child abuse, out of which 4.4% were found to have been victims of child pornography. India is home to almost 19% of World's children population .Are these children offered adequate protection by Indian laws that are enacted to protect children against online child sex abuse? This is the main question that this paper addresses. In India, the Information Technology Act, 2000 and the Protection of Children against Sexual Offences Act, 2012 are two main special laws that deal with offences involving online sex abuse of children. However, the existing laws lack precise definition of many of offences comprising of child sex abuse on internet and/or donot address other emerging cybercrimes targeting children for sexual abuse. For Instance, Section 67B of Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) deals with offence of Child pornography but does not define the term itself. The Protection of Children against Sexual Offences Act, 2012 (hereinafter referred to as the POCSO Act) does not discuss emerging cybercrimes such as cheating by personation or identity theft committed to sexually abuse a child on Internet. This paper elucidates the inadequacies in our extant laws that seek to protect children against online sex abuse in India.

* *Advocate, (BA(Eng Hons), LL.B(D.U), LL.M(King's College, U.K), Phd. Research Scholar (NIU)*

** *Corresponding author: HOD, School of legal Studies, Delhi Metropolitan Education (Affiliated to IP University)*

Keywords: online child sex abuse, online child exploitation, child safety on internet, child protection on internet, sex abuse of children on internet, cyberbullying, child pornography, child grooming

Introduction

Generally speaking, today we all are netizens and not just citizens ! We communicate via apps like whatsapp, watch videos on youtube, listen to music on online channels, do business on tradeindia or indiamart and network through sites like linked in or facebook. Credible sources indicate that the global smartphone users crossed the 1 billion mark in 2012 and were expected to total 1.75 billion in 2014[1]. According to a recent study by Tata Consultancy Services in India, whereas 7 out of 10 children shop online, 76% children have Facebook accounts, and 9 out of 10 children possess a mobile.[2] Reliable statistics point out that India has crossed 100 million Facebook users[3] and studies reveal that India is the sixth largest user of twitter[4]. Through a survey, it was recently found that almost 82% parents help the children below 13 years to set up a facebook account[5]. Whereas parents and educators encourage children to use internet or mobile to equip them with vast information and knowledge resources available online and for communication purposes, little do they realize how hazardous it is to their safety and security, particularly, when they have little or no education on best practices required to maintain their privacy and security in cyberspace.

The World Wide Web is a safe haven for cybercriminals who camouflage their identity via vast anonymity and technical circumvention it offers such as use of proxy servers to commit spoofing where a criminal can easily conceal his true location. They operate singly or in organized gangs to target vulnerable children and commit offences such as cyber bullying, child pornography, child grooming, sexting, sexual harassment, defamation, and related heinous offences. The World Health Organisation defines *'child sexual abuse'* as involvement of a child in sexual activity that a child does not fully understand, and is unable to give informed consent to, or for which child is not developed mentally or prepared and cannot give consent, or that violates the laws or social taboos of society.[6] In this paper, the term 'Online sex abuse' is being used with a flexible and wide connotation and intended to refer to or cover all heinous offences where a cybercriminal sexually abuses a child online including child grooming or child pornography. Broadly speaking, Online child sex abuse can be of various kinds including child pornography, child grooming and some offences may be coupled with other offences such as defamation, identity theft or other crimes committed by offenders with a view to sexually abuse a child. Most jurisdictions would deal with these offenses by enacting provisions in their general criminal laws or by enacting special laws. While criminalizing certain acts as offences, these laws must adequately elucidate the required definitions, ingredients of offence, and scope of its application and term of punishment prescribed for first conviction and a stricter term for repeat offenders.

At the outset, before we analyse the relevant statutory laws, it is alarming to learn the statistics of crime against children in our country. According to the latest report of National Crime Records Bureau following figures are reported-

> "A total of 58, 224 cases of crimes against children were reported in the country during 2013 as compared to 38, 172 cases during 2012, showing an increase of 52.5%. Some IPC crimes have shown a substantial increase during 2013 as compared to 2012. These crimes were kidnapping & abduction (54.2%), procuration of minor girls (51.3%), abetment to suicide (49.3%) and rape (44.7%). Uttar Pradesh accounted for 16.9% of total crimes committed against children reported in the country. The next in order was Madhya Pradesh (14.2%), Delhi (12.4%) and Maharashtra (11.0%)."

What is shocking is that NCRB doesnot categorise data for online sex abuse of children in its reports, particularly cases of online sex abuse of children under IT Act and POCSO. This flags a serious concern and is also an indicator of lack of attention being given to this area of child protection in India both in terms of checking adequacy of its laws, its lacunae and its implementation.

In this paper, we will examine hereinbelow whether various possible threats to children on Internet have been dealt with under extant law in India and made punishable offences and are provisions delineated therein sufficient to protect children on internet in present digital age.

A. Child pornography

This is one of the main threats that children face online today. Till 2009, there was no Section under the Information Technology Act, 2000 that dealt with this offence. After the IT (Amendment) Act, 2008 was passed, Section 67B was incorporated which expressly prohibits, interalia, child pornography and child grooming[7]. According to Section 67B of IT Act, 2000, if any person publishes or transmits material or causes to be published or transmits material containing children in sexually explicit acts in electronic form or creates images text, collects, seeks, downloads, advertises, promotes or distributes content which shows children in obscene or sexually explicit manner, such person is liable to punishment with imprisonment that may extend to 5 years and fine upto 10 lacs and in case of subsequent conviction, imprisonment may extend to 7 years and fine upto 10 lacs. For the purposes of this Section, a 'child' means a person who has not completed 18 years of age. What this provision lacks is the although it connotes and deals with child pornography, it neither mentions the term nor provides precise definition of term 'Child pornography'. Infact, even the Indian Penal Code, 1860 contains neither a Section prohibiting specifically Child pornography nor contains its definition.

Section 293 of Indian Penal Code prohibits sale of obscene objects to a young person but does not deal in child pornography. According to this Section, whoever sells, lets to hire, distributes, exhibits, or circulates to any person under age of 21 years any obscene object such as a book, pamphlet, paper, writing,

drawing, painting, representation, figure, or any other object, if it is lascivious or appeals to prurient interests or if its effect is what tends to deprave and corrupt a person who are likely to see or read it with regard to all relevant circumstances, shall be punished on first conviction for a term that may extend to three years, and fine upto 2000 rupees. And in event of subsequent conviction with imprisonment for a term which may extend to 7 years and fine upto 5000 rupees.

Recently POCSO Act was enacted in 2012 wherein Section 13 of the Act dealt with use of Child for Pornographic purpose. According to Section 13of POCSO whoever uses a child in any form of media (including Programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution for purposes of sexual gratification which includes(a)representation of sexual organs of a child, (b) usage of a child engaged in real or simulated sexual acts (with or without penetration), (c) the indecent or obscene representation of a child shall be guilty of offence of using a child for pornographic purposes.

The explanation to Section 13 explains the term "use a child" includes involving a child through any medium such as print.electronic, computer, or any other technology for preparation, production, offering, transmitting, publishing, facilitation, and distribution of pornographic material.

Section 14 punishes act of using a child for pornographic purpose with imprisonment of upto 5 years and fine and in event of second conviction with imprisonment for a term of upto 7 years and fine. The further subsections of Section 14 prescribe stricter punishments incase person using child for pornographic purposes directly participates in pornographic acts involving penetrative sexual assault or sexual assault.

Section 13 of the POCSO Act deals with use of child for pornographic purposes and brings some clarity on scope and ambit of offence.Infact it enlarges scope of medium from just electronic to television and printed form aswell and clarifies that purpose may be personal or commercial.It enlarges scope to involve simulated acts aswell which are often found in online gaming used to entice children into illegal acts. However, in todays times even semi simulated or morphed images are possible. This Section must be clarified to include semi simulated images by way of an appropriate amendment in Section 13 of POCSO Act. This Section must also be amended to include person who *causes a child* to be used for Pornographic purposes as seen in Section 67B of IT Act, 2000.The definition of child pornography used in POCSO can be made applicable to Section 67B aswell to widen its application. Since pay on demand tv and magazines/newspapers are also available online, scope of application in Section 67B of IT Act, 2000 may also be clarified to include TV and print media available via internet (as seen in definition in Section 13 of POCSO Act).

Further, there is inconsistency in existing law Provisions.Child grooming is punishable with a term of imprisonment of upto three years and fine under POCSO (Section 11 & 12 of POCSO) where as under IT Act, 2000 Section 67B © that deals with grooming prescribes punishment of upto 5 years of imprisonment & fine upto 10 lakhs.These inconsistencies or overlap can be clarified by appropriate amendments.In our view, upto 5 year term should be there and the offence should be non bailable.

Section 15 of POCSO Act provides punishment for storage of pornographic material involving child. According to Section 15, any person who stores for *commercial purposes* any pornographic material in any form involving a child shall be punished with imprisonment which may extend to three years or fine or both. It may be noted herein that even possessing child pornography or seeking, downloading, browsing is also an offence under Section 67B of IT Act, 2000 irrespective of whether purpose is commercial or personal. This inconsistency exists as regards purpose of storage of child pornographic material under POCSO & IT Act, 2000. Further term of punishment differs. Whereas violation of Section 67B is punishable with upto 5 year term of imprisonment, it is only upto three year term for violation of Section 15 of POCSO.

A recent study of 12000 children in India conducted by the Ministry of Women & children led to a shocking finding that 4.46% of children have been photographed without clothes for sexual exploitation purposes. [8] Such problems have been found to exist in tourist places such as Goa where children are often exploited and abused for prostitution purposes[9]. Even if a child is not physically exploited, he can be abused on internet using web camera, videopconferening and other communication applications or tools.Often social networks are infused with malware by criminals such as keyloggers or steganographic files[10], worms which automatically trigger webcamera to start functioning without a child's knowledge or consent.Often children are trapped into luring activity by a criminal to click objectionable pictures of themselves which are obtained by criminal through sms or email or direct webshots from screen.These malpractices not only pose a serious threat to a child's privacy but also may lead to cyber harassment, defamation, kidnapping or even murder.

Hence, punishments need to be made stringent under existing laws dealing with child pornography and inconsistencies in extant law ought to be removed for better deterrent effect on criminals.

Cyber Bullying

This term has not been defined any where in Indian laws.In ordinary parlance, it means giving threats to a child on internet or using a communication device to compel him to do or not to do a particular act in order to mentally harass him/her. When such acts are directed against a child it it is termed as cyber

bullying of a child[11]. The Global Online Behavior Survey conducted by Microsoft recently declared 53% of children between 8 and 17 in India have been victim of cyber-bullying. [12] Most of the incidents occurred on social media and 60% of these took place on facebook. The balance 40% took place in online chatrooms and through mobile phones. Studies have revealed that Cyber bullying can cause depression, irritation, lack of self esteem among children and in critical cases leads to addiction to drugs or even suicide[13].

In order to use a child for child pornography purposes, cyber criminals may use cyberbullying tactics by first luring them into watching obscene videos or images and then use them to produce obscene material .Cyberbullying may even occur to steal personal information of a child to harass him or defame him or illegally obtain financial details such as credit card information to commit phishing[14]. There is no Section dealing with cyber bullying of children under the IT Act, 2000, particularly in context of committing sex abuse. Although Section 66A of IT Act could be said to cover cyberbullying (though not specifically used in context of sex abuse of children) but the ambit and scope of its terms was very ambiguous and it has recently been struck down by the Supreme court for its unconstitutionality.[15] Section 66A of IT Act (before it was struck down) provided that any person who sends by means of a computer resource or communication device any information which is grossly offensive or of menacing character or any information which he knows is false but he sends it to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or illwill persistently by making use of such computer resource or a communication device or email to cause annoyance or to deceive or mislead addressee about origin of such message is punishable with imprisonment for a term which may extend to three years and fine.

In general law, the Indian Penal Code 1860, Section 503 only deals with criminal intimidation without specifically dealing with child sex abuse acts. According to Section 503, whoever threatens another with any injury to his person, reputation, or property or to the person, reputation of anyone in whom that person is interested with the intent to cause alarm to that person or to cause that person to do any act which he is not legally bound to do, or omit to do any act which that person is legally entitled to do as means of avoiding execution of that threat commits criminal intimidation. Section 507 deals with criminal intimidation by an anonymous person which is punishable with imprisonment of upto 2 years in addition to upto 2 years or fine or both as punishment provided by Section 506 IPC in case of criminal intimidation.

Under POCSO Act, 2012, Section 11 prohibits sexual harassment of a child. Section 11(v) addresses one of the situations where a child may be cyberbullied in context of sexual abuse. As per this provision, a person is said to commit sexual harassment upon a child when such person with sexual intent threatens to use, in any form of media, a real or fabricated depiction through electronic,

film, or digital or any other mode, of any part of the body of the child or involvement of a child in a sexual act. Section 12 provides punishment with imprisonment of upto 3 years imprisonment and fine.Another situation which in our view should be added to cover cyberbullying in sex abuse of a child is when such person threatens that child makes himself available for sexual gratification purposes and contacts him persistently through mobile/internet platforms . Whereas Section 11(iv) of POCSO addresses offence of cyberstalking, element of threat to convert it or combine it with cyberbullying is missing. Section 11(iv) states a person is said to commit sexual harassment upon a child when such person with sexual intent repeatedly or constantly follows, or watches or contacts a child either directly or indirectly or through electronic, digital, or any other means. Another observation is that while we don't see a reason to add a mirror provision under IT Act, 2000, it will be perhaps clearer to use correct terms for these acts such as cyberbullying and cyber stalking than to just put them as they currently are under a umbrella term of sexual harassment under POCSO Act.

Selling Cyber Porn to Children

Selling cyber porn to children is an offence in itself.At times misleading ads and popup windows lead a child to inadvertently view adult content.A recent survey points out that while 56% of Indian parents express concern about children being misguided on internet, 42% fear that their children may be exposed to adult content[16]. As explained hereinbefore, Section 293 of IPC prohibits sale of obscene objects to a young person. According to this Section, whoever sells, lets to hire, distributes, exhibits, or circulates to any person under age of 21 years any obscene object such as a book, pamphlet, paper, writing, drawing, painting, representation, figure, or any other object, if it is lascivious or appeals to prurient interests or if its effect is what tends to deprave and corrupt a person who are likely to see or read it with regard to all relevant circumstances, shall be punished on first conviction for a term that may extend to three years, and fine upto 2000 rupees. And in event of subsequent conviction with imprisonment for a term which may extend to 7 years and fine upto 5000 rupees. This should logically apply even to e-books and other digital content via magazines etc which position is yet to be clarified.

Section 67 prohibits publishing or transmitting obscene material in electronic form with a punishment of upto 3 years and fine upto 5 lakhs and in event of second conviction for a term upto 5 years and fine upto 10 lakhs.However, the Section does not provide for any stricter punishment if the sale of adult obscene images or publishing or transmission is made targeting children as users/readers such as new phenomenon of Sexting wherein children or adults send/receive/share obscene messages among themselves. This calls for suitable amendments in IT Act, 2000 incorporating appropriate punishments stricter than general provision when such obscene material is sent to children.

Similarly, Section 67A prohibits publishing or transmitting of sexually explicit act in electronic form and provides punishment of a term of upto 5 years and fine upto 10 lakh rupees and on second conviction imprisonment of upto 7 years and fine upto 10 lakh rupees.But it fails to provide stricter punishment if the offence is made targeting children that is, publishing or transmission of adult images for consumption by children.

Cyber Grooming

Child cyber grooming activity means acts wherein criminal who is a child predator tries to entice or lure children into cyber pornography or other sex abuse activities. Cybercriminals in garb of befriending children set up social media accounts and then gradually entrap children into illegal activates such as sexual harassment or clicking their own selfie pics in obscene form and sending these to the child predator[17].This may be done with malafide intention of making illegal commercial gains or for perverse personal gratification purposes. Though term Cyber grooming is not found in IT Act, 2000, it stands covered by Section 67B©. According to this provision, whoever 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 shall be punished on first conviction with imprisonment that may extend to 5 years and fine upto ten lakhs and incase of subsequent conviction, with imprisonment for a term that may extend to 7 years and fine upto 10 lakh rupees.

Section 67, 67A, 67B excludes any publication made for public good for furthering art, science etc or which is kept for bonafide heritage or religious purpose from ambit of obscene content .Explanation to the Section 67B explains children means a person who is not completed 18 years of age.

Section 11 (vi) deals with cyber grooming and provides that any person is said to commit sexual harassment upon a child when such person with sexual intent entices a child for pornographic purposes or gives gratification therefor. However punishment prescribed for such harassment is only upto 3 years of imprisonment . being such a heinous crime upon a child stricter term of punishment must be provided for such offence under Section 12 of POCSO Act, 2012. Also as pointed out earlier it is inconsistent with term of punishment prescribed under Section 67B which is upto 5 years of imprisonment.

Sexual Harassment

A child may be sexually abused in many other ways apart from child grooming, cyber pornography, cyberbullying or stalking . Some of acts are covered in Section 11 of the POCSO Act, 2012. Section 12 of POCSO Act, 2012 is reproduced hereunder for easy reference:

> "Sexual harassment – A person is said to commit sexual harassment upon a child when such person with sexual intent-

(i) Utters any word or makes any sound, or makes any gesture, or exhibits anu object or part of body with the intention that such word, or sound shall be heard, or such gesture or object or part of body shall be seen by the child, or

(ii) Makes a child exhibit his body or any form or media for pornographic purposes

(iii) Shows any object to a child in any form or media for pornographic purposes or

(iv) Repeatedly or constantly follows or watches or contacts a child directly or through electronic, digital, or any other means or

(v) Threatens to use, in any form of media, a real or favbricated depiction through electronic, film, or digital or any other mode, of any part of body of child or the involvement of the child in a sexual act or entices s child for pornographic purposes or gives gratification therefor.

(vi) Explanation –Any question which involves "sexual intent" shall be a question of fact."

What this Section fails to cover is when a keylogger/ web cam trigger software is intentionally embedded by cybercriminal which unauthorisedloy clicks his pictures without his knowledge or consent invading his privacy.This scenario remains unaddressed. Though Section 66E of IT Act prescribes punishment of upto three years and fine upto 2 lakhs for invasion of privacy of a person, it provides no stricter punishment therein if such invasion occurs in respect of a child. This issue needs to be addressed by the Act by prescribing a stricter punishment for such offences. Moreover, punishment Section 12 prescribes for Sexual harassment is only upto 3 years of imprisonment which is too lenient to deter cybercriminals from committing such heinous acts.

Cyber Stalking

Cyberstalking means to harass someone by following him or her on social media or otherwise through any digital or electronic medium including communication devices.Stalkers try to befriend young children to entice them into cyber pornography or to steal personal information such as personal pictures, or credit card details[18]. Cyberstalking was a punishable offence under Section 66A of the Information Technology Act, 2000 till it was struck down. While major part of Section 66A of IT Act was ambiguous and ought to be struck down as rightly done by the Apex court in the *Shreya Singhal* case, Section 66© was a special law prohibiting cyberstalking and spamming which was also struck down by the same judgement.IT Act, 2000 certainly needs a new provision to prohibit cyberstalking. IPC has provisions that prohibit acts intending to outrage modesty of a woman (Section 509) punishable with a term of imprisonment upto one year or fine or both. For acts that involve criminal intimidation (Section 506) and criminal intimidation by anonymous

communication (Section 507) punishment provided is upto 2 to 3 years imprisonment respectively and Defamation (Section 500) is punishable with upto 3 years of imprisonment, which is not enough deterrence to a cybercriminal. Under the POCSO Act, Section 11(iv) covers sexual harassment involving stalking. According to the provision, a person is said to commit sexual harassment upon a child when such person with sexual intent repeatedly or constantly follows or watches or contacts a child either directly or though electronic, digital, or any other means. Section 12 of POCSO Act makes such act punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine.

In our view, there is need for more stringent punishment for cyberstalking, particularly when such stalking is made targeting a child or a woman under present law.

Identity theft & cheating by Personation

A cybercriminal may garb on another person's identity and cheat a child . He may pose as a young girl or boy and open a social media account using a false picture. Gradually, such person would entice young children by cyber grooming.A cyber criminal may even hack another person's or a child's computer and open fake email and social media accounts by stealing his identity causing identity theft.Such acts are punishable offences. Under IPC cheating by personation is a punishable offence (Section 419) prescribing punishment of upto 3 years and fine or both. Information Technology Act, 2000 contains provisions for identity theft (Section 66C) and for cheating by personation (Section 66D). Section 66C provides whoever fraudulently or dishonestly makes use of electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of term which may extend to three years and fine upto one lakh.

Section 66D provides whoever by means for any communication device or computer resource cheats by personating shall be punished with imprisonment which may extend to three years and fine upto one lakh.However, POCSO does not deal with situation where Identity theft or cheating by personation takes place for sexually harassing a child or for child pornography purposes. A new provision in extant law is the need of the hour to cover such situations with a stricter term of punishment in order to deter cybercriminals from committing such heinous acts.

Immoral Trafficking of Children

Child trafficking for sexual purposes is one of the most rampant forms of child harassment in India[19]. According to statistics relied on by National Human Rights Commission, almost half of children trafficked in India are under 10 years of age.When we speak about Immoral Trafficking, it is not just limited to a physical space any more but can be in a virtual setting aswell. With misuse of

Webcamera, Voice over Internet Protocol, videoconference applications are being rampantly misused by criminals to record and disseminate or share child pornography or indulge in illegal acts of sale, purchase of children or child prostitution. While the IT Act prohibits Child pornography including punishing persons who facilitate abusing children online (Section 67©) and recording in electronic form own abuse or that of others pertaining to sexually explicit act with children, it does not define as to whether Intermediaries such as App providers or website providers who facilitate abusing children online are primarily liable too? Section 79 of the Information Technology Act, 2000 exempts certain intermediaries from liability in certain cases. Section 79 is reproduced hereunder for easy reference.

"79. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him.

(2) The provisions of sub-section (1) shall apply if –

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not –

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if –

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or othorise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation. *For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary"*

According to this Section, an intermediary is not liable for third party information made available by it or temporarily stored or hosted provided intermediary dies not initiate the transmission, select receiver or modify information transmitted subject to observance by it of due diligence. What are the parameters of due diligence and on which yard stick it needs to be measured for compliance is totally ambiguous and not clarified by the Central Government . As a result, the virtual Prostitution haven throng the Social Media platforms or misuse internet on other platforms to carry out immoral trafficking of children.In absence of clear prefiltering laws for sits publishing third party material, unless intermediary is shown to have actual knowledge of such suspicious activity through its website, they are absolved from liability by virtue of Section 79 or unless it is proved that they abet or conspire with the perpetrator of crime.

Second aspect that needs to be analysed critically herein is the old provision in the *Immoral Traffic Prevention Act, 1956(ITPA).* The ITPA Act provides stricter punishment in case of illegal acts of sale, procuring, exploiting any person for prostitution if crimes are committed against children under 16 years.Section 5 of the Act prescribes punishment of upto 7 years which can be extended upto life imprisonment. It makes the people who operate trafficking gangs also responsible for their illegal acts. ITPA does not mention whether this applies only to a physical space or virtual cyberspace aswell. In view of rampant misuse of internet and communication devices for child prostitution purposes virtual child prostitution should also stand covered by this Section which needs to be clarified by suitable amendments akin to amendments made in IPC and Evidence Act in India after passage of IT Act, 2000 . As of now, the meaning of word 'brothel' in Section 5 covers a physical space only. Section 2 (a) of the Immoral Traffic Prevention Act defines "brothel" as *"includes any house, room, conveyance or place, or any portion of any house, room, conveyance or place, which is used for purposes of sexual exploitation or abuse for the gain of another person or for the mutual gain of two or more prostitutes"*. Today, a virtual space can very well be misused as a brothel. The definition of brothel therefore needs amendment to this effect.

Indecent Representation of a Child

Indecent representation of a child by images, drawing, photos, videos is an illegal offence punishable specifically by Section 67B of IT Act, 2000 that prohibits child pornography and Section 14 of POCSO Act for use of a child for pornographic purpose with a term of imprisonment upto 5 years and fine upon first conviction or even stricter punishment. Section 13 that prohibits use of a child for pornographic purposes includes within its ambit commercial or personal use for sexual gratification through any media, print or electronic, television or internet representation of sexual organs of a child, using a child in real or simulated sexual acts or any indecent or obscene representation of a child.

The Indecent Representation of Women Act, 1986 prohibits indecent representation of women through advertisements or in publications, writings, paintings, figures or in any other manner. However, it fails to specify if these provisions apply to the internet aswell. The Indecent representation of women bill, 2012 seeks to incorporate this clarification but is still pending .Further, this Act needs to clarify if the provisions protecting women will also include women below 18 years of age. While Section 3 of the Indecent representation of Women Act prohibits publishing or exhibition of any advertisement which contains indecent representation of women in any form, Section 4 prohibits production, sale, distribution of pamphlets, books, slide, film, painting etc. Section 6 prescribes punishment for upto 2 years and fine for violating Section 3 and 4 of the Act. However, a more stringent punishment must be incorporated if such publication is made with, sold to or sent to a child.

Section 11 of POCSO Act(iii) provides that a person commits sexual harassment if he shows any object to a child in any form or media for pornographic purpose. However, section 12 only provides punishment for the said act with imprisonment that may extend to three years and fine. Even Section 293 of IPC provides punishment of upto three years only (with fine of upto Rs. 2000) for sale, or distribution to any person under age of 21 years any obscene object such as a book, pamphlet, paper, writing, drawing, painting, representation, figure, or any other object, if it is lascivious or appeals to prurient interests. This is not enough deterrence to any cybercriminal and punishments need to be made more stringent.

Hacking Accounts of Minors for Sexual Abuse Purposes

Section 66 of IT Act covers hacking or in other words unauthorized access, and data thefts, but there is no Section in IT Act or POCSO that prohibits hacking of accounts of minors for purposes of sexual abuse.Such provisions must be incorporated in IT Act, 2000 and or POCSO and made non bailable with more deterrent provisions either by way of separate provision or by way of proviso to existing Sections. Moreover, there is also a need to make deterrent provisions for enhancing penalties for repeat offenders, organized crime participants. In some cases such as U.K legislation allows for detention of sex offenders beyond sentence completion. In U.K Crime & Disorder Act (1998) allows courts to extend period of supervision after custodial detention period where a person is suspected to risk of offending further.[20]

Defamation of a Child

Whereas Section 11 of POCSO deals with various forms of sexual harassment, cybergrooming, cyber predation, cyberstalking, cyber harassment, it fails to cover cyber defamation of a child for sexual abuse purposes. Section 500 of IPC makes defamation a criminal offence punishable with a term of

imprisonment of upto 2 years or fine or both. But it does not provide a stricter punishment if a child is defamed involving child sex abuse[21].

Lacunae in Implementation of Existing Law

Though India enacted the Juvenile Justice (Care & Protection of Children) Act to comply with the Convention on Rights of the Child, the Act is silent on giving after care services to victims of online child abuse. The Act also does not specially address those crimes of abuse wherein one child sexually abuses another on the internet. The Act requires establishment of special Juvenile police unit in every district.However, these units have not been set up in most states.In many states there are no special courts to try cases of sexual abuse against children and although every police station is required to appoint 2-3 police officers as child welfare officers, these officers have not been deputed to handle child abuse cases.

Many cybercriminals misuse cybercafé to conduct organized child trafficking or cyber pornography.In India, though IT (cybercafé guidelines) 2011 have been passed, yet no regular monitoring of its functioning is carried out by concerned authorities. This is another major lacuna in enforcement of cyberlaws.

Despite Section 69A of IT Act, 2000 empowers Central Govt to block any website against public order, Computer Emergency Response Team does not proactively block and filter pornographic websites though publishing cyberpornography is illegal in India.Also, though Intermediaries are required to adopt due diligence parameters, there is no clarity on what due diligence requirements are as regards prefiltering of websites wherein child pornographic/adult content may be published or transmitted by a third party.

Section 67C of IT Act puts an obligation upon intermediaries for preservation and retention of information for investigation purposes. According to this provision intermediaries are required to preserve and retain such information that may be specified for such duration and in such manner and format as Central government may prescribe. However, as on date central government has not prescribed any guideline for minimum log duration that must be preserved by intermediaries and produced when required for investigation purposes.

Although Section 20 of the POCSO Act puts the obligation on media, studio and photographic facilities to report content on web which contains child pornography to Special Juvenile Police Unit or to local police, but this limits it to acts punishable under POCSO .It does not cover acts punishable under IT Act, 2000 and IT Act itself has no such provision . Section 21 of POCSO provides punishment for failure to report under Section 19 and 20 of POCSO Act with imprisonment upto 6 months or fine or both. Appropriate amendment putting

a similar obligation on intermediaries under IT Act, 2000 is also warranted. Similarly, obligation to report to police in Section 19 of POCSO Act rests on any person (including a child) who has apprehension that an offence is likely to be committed or has knowledge that such offence has been committed under POCSO Act . Such provision should also be incorporated by way of an amendment under the IT Act, 2000.Such cooperation networks are commonly seen and have been quite successful in U.K & U.S .In *Operation ore* UK based credit card companies tracked identity and location of people who used credit cards to buy child pornographic materials from a website Landslide inc based in the U.S[22].

India is a signatory to the Convention on the Rights of the Child and has enacted various special laws to comply with its obligations. However, from the abovesaid, it stands clear that our laws are blatantly inadequate to deal with rising diverse online sex abuse forms that pose as a threat to our children on internet. Inadequacy exists both in our laws/policies and also its effective implementation. In India, National Policy for Children 2013 envisages children ought to be given a safe and secure environment.The Ministry for Women And Child Development is responsible for implementation of the policy and responsible for formulating National plan of Action[23]. The National Commission for Protection of Child Rights and State Commission for Protection of Child rights are responsible to ensure principles of this policy are observed.In many cases State Commission is not functional or lacks resources and due appointments of experts to form the panel or child welfare committee is long overdue. As a result effective implementation of law suffers[24]. The Integrated Child Protection Scheme has also been launched but it doesnot deal with protecting children against sex abuse online . Combating online sex abuse of children has not so far received attention it deserves in our country. As a result, there is a lot to be undertaken in terms of identification, reporting, legal recourse, after care and rehabilitation of children who are victimized online for sexual abuse. Also, India is not a signatory to a Cybercrime Convention, in absence of which investigating cross border cybercrimes which target children meet with little success and are at mercy of investigating authorities abroad who may or may not choose to offer required cooperation[25].Therefore, tracing a cybercriminal abroad is faced with several hurdles, and extradition and prosecution of cybercriminal in India may not be possible in many cases. Also, the police personnel require proper training in cyberlaws and cyber forensics for collecting and preserving electronic evidence for effective prosecution and our law enforcement including judges need continuous training in this area as a cyber criminal is technically equipped and knows ways and means to circumvent the law.Our laws need to keep pace and therefore suitable amendments will be necessary from tume to time to strengthen legal regime to protect our children in cyberspace.

Conclusion

Protection of children against sexual abuse on internet is an imperative global concern today. There are glaring inadequacies in our existing Indian laws that protect children against sexual abuse online which must be addressed immediately to amend the extant laws appropriately and strengthen child safety and security in online world.We need a multi-stakeholder approach wherein legislators, parents, educators, NGOs, law enforcement, private sector, Internet service providers work towards protecting children on internet in a PPP model (Public Private Partnership model).The inadequancies in extant law ought to be removed, including inconsistencies and for effective implementation of laws, it is necessary that government bodies draft appropriate policies and schemes to prevent and combat online sex abuse of children followed by its regular monitoring and effective coordination by the paraphernalia /machinery Government has created for the purpose.

Notes

1. See more at: *http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536#sthash.1efnEHEz.dpuf*
2. Tata (2014), TCS GenY 2013-14 survey reveals urban teenagers are hyper-connected. Retrieved from *http://www.tata.co.in/media/releasesinside/TCS-GenY-2013-14-survey-reveals-urban-teenagers-are-hyper-connected.*
3. Social Media 2014 statistics- an Interactive Infographic! Retrieved from Digital Insights at *http://blog.digitalinsights.in/social-media-media-users-2014-stats-numbers/05205287.html.*
4. Semiocast (2012) Twitter reaches half a billion accounts, more than 140 million in U.S Retrieved from *http://semiocast.com/en/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US*
5. Medhashree Dutta,TNN (2014,Jul 13) Under 13 kids social networking sites okay? The Times of India, *http://timesofinia.indiatimes.com/life-style/relationships/parenting/Under-13-kids-using-social-networking-sites-okay/articleshow/3689245*
6. WHO. Guidelines for Medico legal care for victims of sexual violence , retrieved from *http://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf*
7. See section 67B© IT Act, 2000.
8. Ministry of Women and Child Development, Government of India (2007) Study of Child Abuse, India 2007, Retrieved from *http://wcd.nic.in/childabusing.pdf*
9. ECPAT (2005) ECPAT (End child prostitution,child pornography and trafficking of children for sexual purposes) Report, *www.ecpat.net/sites/default/files/India%201st.pdf*
10. Files which are hidden and camouflaged. For example a harmless music file may infact be an obscene video but appear to be a music file.
11. Rumor spreading, trolling, that is (to send abusive statements online) and happy slapping, (that is sending a recorded clip of child abuse through social media) are

some common forms of cyber bullying. Hinduja, S, Patchim J. (2009) Bullying beyond the school yard: Preventing and responding to cyberbullying. USA: Thousand Oaks, Corwin Press.

12. Microsoft Safety and Security center, *http://www.microsoft.com/security/resources/research.aspx*
13. Dr. Srivastava, S. (2012), Pessimistic side of information and communication technology, cyberbullying and legislation laws Internet Journal of Advance in computer Science and Technology 1(1) pp. 14-20.
14. A term given to a financial crime wherein personal information is stolen by a criminal to unauthorisedly debit moneys from accountholder's account.
15. See *Shreya Singhal v UOI case*. Section 66A of It act lacks guidelines, *http://indianexpress.com/article/india/india-others/no-guidelines-prone-to-abuse-sc-criticises-sec-66a-of-it-act/*
16. Indian parents wary of kids getting hooked online: Survey(2011,June 23) Indo Asian news service at *http://gadgets.ndtv.com/internet/news/indian-prents-wary-of-kids-getting-hooked-online-survey-225908*
17. Selfie pics can render childrenvulnerable to child predators (2014,july 16) Retrieved from *http://www.ksat.com/content/pns/ksat/news/2014/07/16/-selfie-pics-can-leave-children-vulnerable-to-predators.html*
18. See Childprotectionindia.com- A website by Lex cyberia dedicated to spreading awareness on threats to children in cyberspace and best practices to safeguard their privacy. Download also App on cyberlaws & IT Act,2000 by Lex cyberia (available on Android platforms for free).
19. Sen, S. (2005), Trafficking in Women & Children in India, New Delhi, India : NHRC.
20. Julia Davidson, Internet Child Abuse, edited by Julia Davidson, Petter Gottschalk, chapter 1 @pg 18.
21. Section 66A of IT Act dealt with defamation as offence but was recently struck down as unconstitutional by the Supreme Court in the *Shreya Singhal case*.However even Section 66A did not dilineate defamation of a child for sexual abuse as an offence.
22. Child porn suspects blame fraud(2007,May 10)BBC News Retrieved from *http://news.bbc.co.uk/2/hi/uk_news/6641321.stm.*
23. Ministry of Women & Child Development, *www.http://wcd.nic.in/*
24. Human Rights Watch, Breaking the Silence,Child Sexual Abuse in India, 2013 *http://www.hrw.org/sites/default/files/reports/india0113ForUpload.pdf*
25. Seth Karnika, Protection of Children on Internet,Universal Law Publishing company, 2015.@pg. 98.