Policy brief series: No. 21; 2014 July-August

Centre for
Legislative Research
and Advocacy

Policy Brief for Parliamentarians

Cyber Child Abuse:
Measures to prevent and fight it

Introduction

The internet world has become an indispensable part of our day to day lives. Children, in particular, are actively indulging themselves on the internet for the purpose of education and social interaction; at the same time, they are susceptible to fall prey to online predatory criminals. Educating the children about practising safe online behaviour in order to enjoy the gifts of web world and safeguard from the potential danger of online criminals is of pivotal importance. At the same time, it is important that the government, together with the epistemic community, school teachers, parents and children should actively work to build a safe environment for the innocent minors as well as mitigate and combat the cyber paedophiles.

The purpose of this policy brief is to get to the heart of the matter of online child abuse and highlight the various facets and aspects of this issue to the Parliamentarians to better comprehend, prevent and combat the growing menace of online child abuse (which has the potential to threaten our children - 39% of Indian population, at present as well as in future) with strategically crafted policy steps. This brief is a small step in this direction.

Cyber Fact File: India

- Became the 3rd largest internet user in 2012 (Internet World Statistics 2012).
- Will have 519 million internet users by 2018, growing at a rate of 25% per year – thanks to decreasing mobile prices, increasing smart-phone usage, faster bandwidth and rising internet content and services.

Cyber Crime Fact File: India

- India features in the top 20 countries with maximum percentage of cyber crime.
- NCRB reports **122.5%** rise in cyber crime from 2012 to 2013; **76%** were obscenity + hacking related.
- Of the 5693 cyber crimes, **1203** were the reported online pornography related cases (which is 100% increase from 2012-2013) and about **737** people were arrested due to online obscenity related crime.
- **56.7%** (1190/2098) of the total cyber criminals were noted in the age group of 18-30 years, **34.4%** (722/2098) aged 30-45 years, and **47** of the cyber criminals were juveniles.

Tata Consultancy Service (TCS) Generation Web 2.0 2009 survey illustrates:
(out of 13738 Indian students in metro and mini-metro cities)

- ***41%*** *preferred Google as a source of information over TV, newspapers, library, etc.*
- *Majority students accessed internet from home computer Vs cyber cafe, mobile, etc.*

As per TCS Youth Survey 2014 across India:

- ***56%*** *rely on internet as source of information.*
- ***75.73%*** *students have facebook accounts and consider it a preferred site over Google+*
- *Most students access internet via home computer (**78.82%**) and mobile phone (**10.96%**) Vs cyber cafe, tablet.*
- ***1 in 2*** *students spend more than an hour on internet.*

NOW, figure this!

McAfee's 'Secret Lives of Indian Teens' surveyed 1500 Indian parents and teens in Indian metropolitan cities and found that (Anon 2012):

- Children are vulnerable to online crimes and 47% felt that online nudity disturbed them.
- 1 in every 4 teens has been victimized by online predators.
- 53% of Indian teens have seen sexual content online mistakenly by spams and advertisements; while majority of parents trusted their children to not access nudity online (79%).
- 35% teenagers knowingly see obscene materials online, whereas only 14% parents are conscious about this.
- 20% adolescents view nudity on the web daily and yet 32% parents thought that the teenagers view them only a couple of times a year.
- Parents are not always available to check the online activities of their teenagers (53%) and 61% feel they are not as tech savvy as their adolescents, thereby highlighting the digital cum generational gap that exists between the Indian parents and minors.

Analysis of facts & figures:

Internet penetration is so fast that the internet access exceeds skills and socio-cultural adjustment and children's internet use surpasses parent's use; in short, digital cum generation gap has widened.

Many cases of teenagers' exposure to online pornography and their victimisation often go un-reported, because lack of awareness or generation gap with parents. So even though the figure of 'reported' or 'registered' online obscenity related cases, according to NCRB (2014), is very less compared to the number of reported conventional crimes, the actual figure could be much more.

Cyber safety of children matters: But why?

The internet has, beyond doubt, given innumerable and invaluable opportunities to learn, grow, and entertain children worldwide. Unfortunately, the online world also offers ample scope for online predators to target children (regarded to be below 18 years, as per UNCRC) because they are innocent, vulnerable, lack maturity and therefore, become an easy prey to online

sexual abuse. Also, the web is anonymous, cost-free world which offers easy access to children. Children have to experience sexual solicitation, obscene content, cyber harassment and cyber bullying, etc.

The Online sexual exploitation of minors has developed into "a serious problem" (End Child Prostitution and Trafficking (ECPAT) 2001) which is no less than epidemic.

Online sexual grooming is spreading like wildfire, wherein:

- Cyber paedophiles aim to 'groom' the teenagers by winning the confidence of the innocent minor, encouraging them to post their personal information and photographs online, enticing them to indulge in online sexual activities for the purpose of personal and financial gain.
- Eventually, they end up blackmailing and humiliating the victimised child (for money, pleasure, for instance) or circulating the victim's pornographic video over the web, thereby causing great embarrassment and tension to the young victims and his/her family.

Obscene Online Content has exposed them to experiences that could:

- Gravely affect the psychological health of children like insomnia, mood swings, depression, suicide, etc. (on the extreme side of the spectrum), and affect the sexual and emotional state of the child.
- Make the children even more vulnerable to sexual harassment, cause them to behave in a sexually problematic way or may want them to entice their counterparts to engage in pornography online (Jones & Quayle 2005; Taylor & Quayle 2004).
- Lead to self-victimisation or self destructive behaviour too (Longo 2004).

Parenting has become incredibly challenging due to the fast pace of technological innovation:

- The primary stakeholders, including parents, teachers and carers are fairly new to the risky side-effects of new-age technologies.
- The primary stakeholders in India are not adequately empowered and equipped with education and skills required to effectively protect the children from potentially harmful and sexually explicit content on the web world.
- There have been number of cases when due to ICT, social networking sites, etc. Indian children have been abused online or blackmailed; so much so, in extreme cases, they have even committed suicide.
- Societal pressure and fear of victimisation by law enforcement authorities are reasons responsible for the fear parents feel in reporting child sexual abuse – whether online or offline.

Our current context:

Lack of Data: One of the most pressing challenges one faces when analysing the pertinent issue of online child abuse is serious dearth/lack of state commissioned research which could offer scientific, valid statistics on number and nature of age-wise and location-wise use of internet by children as well as record of online child abuse, children's exposure to sexual material online, etc.

IT Act: Recognising the urgent need for bringing the laws to regulate the new-age technology crimes was felt in India, as a result of which the IT Act, 2000 has provided in section 67 for punishing obscenity in electronic form. The IT Amendment Act 2008 (ITAA 2008) encompasses section 67B in which electronic depiction of children in sexually explicit acts as well as online child abusing are a punishable offence. In subsection 2 (ha) 'computer network' entails 'communication device' like cell phones. The IT Act should be applauded for coming up with a technology-neutral law and the ITAA 2008 for making the offence under section 67B cognisable and non-bailable, thereby recognising the seriousness of electronic crimes against children. Yet, there are some limitations of the IT Act when it comes to tackling online child abuse. For instance, the definition of 'child' does not include **real and virtual children and also adults appearing to be children**. Definition of online child abuse is not explained to include online sexual grooming of minors (i.e. enticing and soliciting the child for further offline abuse, intentional or unintentional access to sexually explicit, harmful content by minors both intentionally and otherwise), and circulation or reception of online child sexual abuse images (Mathew 2009).

Law Enforcement & Jurisdictional issues: While the Indian IT Act has given a provision for extra-territorial jurisdiction to law enforcement agencies, however, since India has not signed any reciprocation and extradition treaties with any international conglomeration of countries to combat cyber crimes like child abuse from online sexual harassment, cyber bullying, etc., cyber criminals often take advantage of this very legal gap.

The Indian government has not yet taken a proactive measure in this regard, as opposed to the US's law enforcement officials who tempt potential sex offenders to contact minors online via sting operations, for instance. The UK has collaborated with Europol and the Virtual Global Taskforce (VGT) that works with online service providers to mitigate the occurrences by aggressively being on a lookout to check online child sex abusers and has convicted them too.

MHA's Advisory: At the level of the State, the Indian Home Ministry in its advisory (MHA 2012) issued, in 2012, to the Indian states has provided many valuable suggestions to prevent and combat internet crimes against the minors like educating and training of Indian Police, Prosecution and Judiciary about ways to effectively deal with cyber crimes against minors. The

document also touches upon the need to educate and empower children, parents and teachers as well as other relevant state and non-state actors with correct knowledge to address the problem at hand. However, the document clearly states that the measures encompassing the advisory letter are **only indicative** and it does not mention about holding specific departments accountable for implementation of recommendations dealing with online crime against children. Also, the aforementioned document points out that processing of digital evidence in Computer Forensics Laboratories takes up a long time, because of which digital footprints are often lost. There is no concrete timeline based action plan to check this and the states authorities are merely asked to come up with their own central and regional Forensic Laboratories as per their convenience.

India needs to plan and execute effective, valuable child-centric solutions to both protect and empower the children from online sexual harassment threats and also check and mitigate the impact of the anti-social, illicit activities of the online predators.

Measures to prevent and fight the issue: Because it is time for action!

India ratified UNCRC's convention which outlined the four important child rights which every state must try to provide to minors – including child's right to survival, development, protection and participation. Children constitute 39% of India's population (Census 2011) out of which, 84% belong to the tender impressionable age of 0-15 years; chances are that these children will engage in various ICT devices and therefore, India needs to make it a national priority. The problem of online crimes against children is clearly one of the most perilous challenges of the present day and age where the government must take the lead to protect the children from online and offline predators. Elimination of internet crimes from the web world is a near impossible task; however, the following recommendations could help prevent and combat cyber child abusers and facilitate mitigation of negative effects of the online threats because there is no single magic-wand solution that could prevent or cure the problem of online abuse of children.

What the Government is recommended to do at national level

- ✓ ***Need for evidence based, child-sensitive policy:*** Clearly, the statistics provided by NCRB and McAfee are inadequate to give an actual picture of the problem at hand. Setting up a multi-stakeholder forum or a commission encompassing the government, the industry, the epistemic community as well as parents, children and school teachers, on the lines of UK Council for Child Internet Safety, which would scientifically conduct empirical research to report on the number, nature and risks of online child abuse, develop an effective system or institution to check it, and design an impactful and sustainable strategy at all levels should be useful.
- ✓ ***Educate the primary stakeholders (including children, parents and teachers):*** The best way to empower children, parents and schools against online predators is by educating them to spot any potential online hazards and ways to deal with those risks by:
  - ***Developing a resource booklet and a website for cyber-safe guidance:*** The government should, together with the industry and other stakeholders of the society, devise a valuable guide for children, parents and teachers to educate them about measures to tackle internet crimes against minors with practical solutions (in vernacular language, since India is a diverse country) to the victims of online abuse (ITU 2009; UNICEF 2011).
  - ***Conducting online safety workshops:*** Instruct all educational institutions to conduct workshops for children, right from primary classes, every year that would educate them about the potential cyber risks; and be made to inculcate cyber-safe habits (ITU 2009; UNICEF 2011).
  - ***Nationwide campaign:*** Run a massive, nationwide campaign with the help of the print and electronic forms of mass communication to make everyone aware of the problem at hand (ITU 2009; UNICEF 2011).
  - ***Including internet safety in the school curriculum & establishing 'Online Safety Day':*** *This will make cyber safety an integral life skill thereby empowering children to safely manoeuvre in the web world.*
  - ***Promoting the use of technological software and devices under parental control:*** This could make the internet safe for use by children such as filter software, spyware software by parents and the use of online safety games to train children in web-safe practices, etc.
- ✓ ***Set up 24 hour Hotline and Rehabilitation Centres:*** In order to make a provision for 24 hours specialised counselling service for those children who fall prey to online child abusers (ITU 2009; UNICEF 2011). A strong stance by the government, to check societal harassment would facilitate the recovery and reintegration of child victims into communities and families. In this regard, establishing partnerships with existing mental health experts, who specialise in counselling children might be useful.
- ✓ ***Collaborate with Internet Service Providers and other Internet Industry sectors:***
  - ***Block search results of online child abuse terms:*** The government should provide the Internet

Industry with a range of child abuse related 'blacklisted' terms, so that in case someone types those words, the Internet Service Providers should not present them as a search item. This kind of facility can come up only with the help of collaboration between the Internet Industry and the government. The direct result of this would be to create difficulties, blockages in accessing child abuse sources and resources on the internet.

- ***Filter the web content and target child abuse/ child pornographic websites:*** The Internet Service Providers and Government should make parenting, upbringing of children easy and in fact, less complex for parents, guardians, teachers and carers.

✓ ***Recommendation for the IT Act:*** There should be clarity about how law of the land could possibly be applied to matters of cyber crimes against teenagers (Mathew 2009). Also, the laws of the country have to keep up with the pace of technology:

- ***Child's definition:*** Section 67B of the ITAA deals with the issue of online child pornography; however, the term child is not defined to include real and virtual children and also adults appearing to be children.
- ***Online child abuse should encompass:***
  - Online Sexual Grooming of Minors in which online enticement, circulation of pornography whether from adult to child or child to child for further offline abuse, encompassing both child-to-child grooming as well as adult-to-child grooming.
  - Child's intentional or unintentional access to sexually-explicit content online via misleading domain names, pop-ups or other means during otherwise innocuous activities.
  - 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.
  - Online access to real time images of minors being sexually abused (via web cam, etc).

✓ ***Law Enforcement Agencies:*** Our law enforcement agencies are not adequately prepared to check and defend the minors through traditional means of policing. Law enforcement establishment should:

- ***Be empowered with technical training in computer forensics investigation*** – in all the four metropolitan cities of India to begin with – to successfully identify and combat internet related threats against the young people, in a time bound manner (in order to not lose the digital evidence).
- ***Be trained to treat child sensitively and compassionately,*** which will help victimised child and her/his parents to willingly report online abuse to the law enforcement authorities and would not garner any fear of further victimization by the criminal justice system.

✓ ***Regarding the MHA Advisory:*** As stated earlier, the MHA Advisory note appears very thoughtful; it should be made more robust by establishing:

- ***A concerted, well-coordinated monitoring mechanism or institution to ensure accountability*** for the MHA's policy recommendations. Strong messages should be sent out by the government ministries (including Ministry of Science & Technology, Women and Child Welfare, and Home Affairs) 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 (Mathew 2009).
- ***A review committee*** by the MHA to ensure that any of the limitations of the current advisory are adequately addressed in the next policy, considering the need of the day.

What the Government is recommended to do at International level

✓ ***Web world is a borderless, anonymous world:*** Cyber criminals look for ways to exploit the weaknesses in the law and enforcement practices of countries to achieve their objectives. In order to effectively combat the anti-social, illegal activities of online predators and to prosecute them across the border, it is important:

- To have arrangements made for cooperation in investigating and responding to the cyber threats like online pornography effectively (ITU 2009; UNICEF 2011).
- To coordinate with agencies like the VGT and Europol and join the combat against online child sexual abuse.
- In this respect, we may initiate a forum at South Asian level to begin with.
- To promote arrangements 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.

Conclusion

Children are vulnerable to the exploitation of cyber paedophiles and, therefore, a strong collective response is required at national and international levels, in order to successfully check and mitigate the hazardous risks of

the web world. The Indian Government together with the support of the epistemic community and internet industry should design policies and come up with a holistic, timeline based action plan to prevent and combat online sexual offenders and cyber stalkers from harming the minors in India. At the same time, there is an urgent need to engage with children, on part of the parents, teachers and psychologists to offer a customised solution to educate the young Indian minds to practise safe online behaviour, and tackle the online predators effectively and enjoy the ocean of knowledge, opportunities and entertainment of the web world.

Acknowledgements

CLRA and PGC would like to offer gratitude to Smt. Vandana Chavan, MP, Dr. T.N. Seema, MP, Smt. Kushal Singh (Chairperson of NCPCR), Dr Rumi Aijaz of ORF, Mr Prashant of SFLC, and the entire team at CLRA for their very informative feedback and support in developing this policy brief, and Ashish Singh for drawing the cartoon sketch exclusively for this policy brief.

Selected References

Anon. (2012) McAfee Survey Reveals A Growing Digital Divide Between Indian Teens And Parents. 22 November 2012. IndiaPRwire. See: http://www.indiaprwire.com/pressrelease/security/20121122137430.htm

BusinessWeek/Symantec (2009) Top 20 Countries Found To Have The Most Cyber Crime. See: http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

ECPAT (End Child Prostitution and Trafficking) (2001). See: http://www.focalpointngo.org/ ngonews.htm,

Internet World Statistics (2012) Top 20 Internet Users of the World. See: http://www.internet worldstats.com/top20.htm

ITU (2009) Guidelines for Policy Makers Children Online Protection. See. http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/policy_makers.pdf

Jones, V. and Quayle, E. (2005) Protecting Children from Online Sexual Exploitation, Save the Children, Denmark, September 2005. See:http://www.childoscope.net/2009/httpdocs/publications/cddea67ce2be65c6c725b6513e782bcf.pdf

Longo, R.E. (2004) Young people with sexual behaviour problems and the Internet. In M. Calder (Ed), Child Sexual Abuse and the Internet: Tackling the New Frontier. Dorset: Russell House Publishing.

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

MHA (2012) Ministry Of Home Affairs, Government of India Issues Advisory On Preventing & Combating Cyber Crime Against Children, National Legal Research Desk. See: http://nlrd.org/childs-rights-initiative/latest-advisories-notifications-child-rights-initiative/ministry-of-home-affairs-government-of-india-issues-advisory-on-preventing-combating-cyber-crime-against-children

National Crime Report Bureau (NCRB) (2014), 2013 Cyber Crimes. Chapter18. See: http://ncrb.gov.in/CD-CII2013/Chapters/18-Cyber%20Crimes.pdf

Taylor, M. & Quayle, E. (2004) Abusive images of children. In Medical and Legal Aspects of Child Sexual Exploitation. Sharon Cooper, MD; Angelo Giardino, MD, PhD; Victor Vieth, JD; and Nancy Kellogg, MD. (Eds). Saint Louis: GW Medical Publishing.

TCS (2009) TCS Generation Web 2.0. See: http://www.tcs.com/sitecollectiondocuments/tcs_news/tcs_pr_generation_web2.0_survey_07_09.pdf

TCS (2014a) Youth Survey 2014. See: http://www.tcs.com/SiteCollectionDocuments/2013-2014-GenY-Survey-TCS-0614.pdf

TOI (2014b) Small town India turns out to be hub of cyber crime – Times of India. 2014. See: http://timesofindia.indiatimes.com/tech/tech-news/Small-town-India-turns-out-to-be-hub-of-cybercrime/articleshow/37976522.cms

TOI (2014) India to have 519 million mobile internet users by FY18, Morgan Stanley. See: http://times of india.indiatimes.com/tech/tech-news/India-to-have-519-million-mobile-internet-users-by-FY18-Morgan-Stanley/articleshow/36656019.cms

UNICEF (2011) Child Safety Online Global Challenges and Strategies. See: http://www.unicef.org/ malaysia/2011-UNICEF-IRC-Child-Safety-Online.pdf

Policy brief series: No. 21; 2014 July-August

Cyber Child Abuse: Measures to prevent and fight it

Author:
Shweta Singh*

Editorial Inputs:
Mahima Taneja (CLRA)
Cartoon by Ashish Singh

For more information, contact: Centre for Legislative Research and Advocacy (CLRA), F-29, B.K. Dutt Colony, Jor Bagh, New Delhi-110003, Tel: 91-11-24640756, E-mail: info@clraindia.org, website: www.clraindia.org

*Shweta Singh is Research Intern at CLRA, and currently is a student of Master of Public Policy at Edinburgh University 2013-2014.

Supported by: Parliamentarians' Group for Children (PGC)

Published by:

Centre for Legislative Research and Advocacy (CLRA), an organisation of expertise in parliamentary development and legislative advocacy is the hosting/implementing organisation of the PGC, IMPF and PG-MDGs.