Child Online Protection in India

unicef
unite for children

Child Online Protection in India

स्तुति कक्कड़
Stuti Kacker
अध्यक्ष
Chairman

भारत सरकार
GOVERNMENT OF INDIA
राष्ट्रीय बाल अधिकार संरक्षण आयोग
NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS
नई दिल्ली–110 001
New Delhi–110 001

Foreword

Child Online Protection is a global challenge which needs to be undertaken urgently. Today's children have wide access to internet via mobile phones, laptops, tablets, desk tops, and other devices. They are fascinated by such devices and scouring the internet for all types of information. In India, it is estimated that about 134 million children have mobile phones. The number is growing by leaps and bounds. Also, with broadband expansion, these children will have faster access to internet by 2017. This phenomenal growth will provide opportunities to the children of the country to access and share useful material for learning purposes. But on the other hand, lack of digital literacy and online safety measures will also expose these children to hazards of cyber bullying, sexual predation and other crimes. In order to curb the menace, all stake holders, Government Ministries/Departments, law enforcement agencies, civil society organizations, private corporations etc. should join hands while enlisting cooperation of other countries.

The National Commission for Protection of Child Rights (NCPCR) is constantly endeavoring to protect children from abuse and to ensure that their rights are protected. In this effort, it is heartening to note that the "CHILD ONLINE PROTECTION in India-an Assessment" by UNICEF addresses all relevant issues in the report, like: expansion of ICTs and the internet in India; online risks and threats, and their impact on children; structures; mechanisms and capacities and analyses existing Indian laws and policies. The Report suggests appropriate interventions. The task was not easy but the efforts made by the UNICEF and associated organizations/individuals who have contributed, are praiseworthy.

This Report is an important step in the direction of child online protection and safety and will go a long way in improving child online protection measures in our country.

(Stuti Kacker)
19th September, 2016

5वां तल, चन्द्रलोक बिल्डिंग, 36, जनपथ, नई दिल्ली-110 001
5th Floor, Chanderlok Building, 36, Janpath, New Delhi–110 001
दूरभाष/Ph. : 011-23478212, 23731583, फैक्स/Fax: 011-23731684
Web: www.ncpcr.gov.in

NASSCOM®
FOUNDATION

Foreword

I still remember getting Diwali crackers for my daughter with a fair warning that while they add to a lot of fun, they may harm my child just as much. I wish our Computers, Mobile phones and other digital devices also came with such warnings, for the scars the internet can leave on the impressionable children of this age, can take a lifetime to heal.

Internet is a great tool when used wisely and can really enhance a child's learning but at the same time it puts an unattended child at risk of getting exposed to real world (rather adult world) dangers of online fraud, cyber-bulling, racism, pornography and violence.

Child online protection is a global need and is taken very seriously in a lot of countries but sadly India is a little late to even realize it. We aim to become a technology powerhouse with campaigns like Digital India and Skill India but this is one area we are seen lacking.

NASSCOM Foundation as the 'Technology for Good Partner' to this publication, is committed to the cause and promises to bring in the IT industry expertise in trying to present our country's children with a secure and safe online experience. The Foundation also works in partnership with the Government of India to train people from underserved communities on digital literacy under the National Digital Literacy Mission and going forward will include an additional section on basic online safety for teenagers and young adults.

I am glad that UNICEF has brought together the right set of people to address this issue and this publication will help guide us all to work together to make the cyberspace safe for India's Generation Z.

(Shrikant Sinha)
CEO, NASSCOM Foundation

Pandit Uma Shankar Dikshit Marg, Diplomatic Enclave,
Chanakyapuri, New Delhi, Delhi 110011

Preface

The rapid spread of information and communication technologies (ICT) in India has created a wealth of opportunities for economic growth, the spread of knowledge, lowering the cost of education, social networking, democracy and better governance and accountability. While India's Internet coverage is still lagging behind that of other BRICS countries, especially among poor, rural and remote people, the country is rapidly catching up and offers the largest untapped market for Internet access, especially through smartphones.

While access to ICT and participation in the online environment are rightly priorities for the Indian Government, online risks have received relatively less attention. Cybercrime statistics focus on commercial online fraud and political radicalization. The risks of online abuse and exploitation of children have received much less attention and are not included in the National Crime Records Bureau statistics as a separate category. India's ability to protect children from online abuse and respond effectively to the dissemination and consumption of online child sexual abuse materials (aka child online pornography) falls far short of meeting existing needs. In fact, there is a widespread lack of awareness among parents, teachers, the police and policymakers of the growing and ever changing risks of child online abuse and exploitation. Legislation, mechanisms and services are inadequate to respond to these threats and have to be updated and strengthened. Given the global nature of the Internet, there are particular challenges regarding the lack of effective coordination between law enforcement branches, between law enforcement and ICT companies and across national boundaries.

UNICEF commissioned the assessment of child online protection in India to better understand the online risks faced by children, to identify gaps in legislation, to ensure removal of harmful online materials, to support investigation and law enforcement and to identify services for child victims of online exploitation and abuse. The aim of the study was to identify priority interventions for the Government, ICT companies, non-governmental organizations and international agencies. The study provides a comprehensive overview of the current situation of child online safety based on the available data. It is a resource that should help any organizations working on various aspects of child online protection to enhance their awareness of existing gaps and understand both where to improve their own interventions and where to strengthen collaboration and coordination with other stakeholders.

The assessment distinguishes broadly between two kinds of child online abuse: (a) harmful and abusive online behaviour between children; and (b) online sexual exploitation of children. While most of the former does not constitute a criminal offence and should not be criminalized, there is a need to embed efforts to protect children in a wider digital citizenship approach that gives equal

weight to the equitable provision of and access to ICT, to participation in the Internet and to protection of children from harmful and abusive content. The second dimension concerning online sexual exploitation of children requires robust action, particularly from law enforcement agencies and ICT companies.

In the course of this assessment, the consultants identified a small group of experts and professionals who are knowledgeable and passionate about online safety. This group forms a valuable resource pool for any effort to protect children online.

We hope that this report will receive wide circulation and will lead to concrete actions by all stakeholders so that children across India are able to enjoy the benefits of the Internet without facing abuse and exploitation. UNICEF is committed to working with other actors to make the digital ecosystem safer for all children in India.

(Louis-Georges Arsenault)
Representative, UNICEF
New Delhi, September 2016

Acknowledgments

The authors would like to acknowledge the important and timely contributions of the informants from the Government, industry and civil society. Without their valuable inputs and keen insights, this report would not have been possible. A list of informants is included in the annex.

We would like to make special mention of Vidya Reddy of Tulir, cybersecurity expert Rakshit Tandon and cyber law expert Karnika Seth for extending valuable support throughout the process of enquiry and drafting.

We are grateful to Kumar Alok from the Ministry of Home Affairs; Rina Ray from the Ministry of Human Resource Development; A S Kamble and Rakesh Maheshwari from the Department of Electronics and Information Technology; Subho Ray of the Internet and Mobile Association of India; Deepak Maheswari of Symantec; Nand Kumar Sarvade of the Data Security Council of India; B Bhamathi (retd. Indian Administrative Service); and P M Nair (retd. Indian Police Service).

We acknowledge the contributions of technical and legal experts and representatives of the corporate sector and civil society who provided information and perspectives for the research and analysis through interviews and consultations in February and April 2016. Also, we would like to thank all the experts who actively participated and contributed to the expert consultation on Child Online Safety in India hosted by UNICEF in New Delhi on the 8-9 of April 2016 as they supported the endorsement of the key findings of this report and the development of the key recommendations.

We would like to thank Sonia Livingstone of the London School of Economics, Susie Hargreaves of the Internet Watch Foundation, Kate Sinnott of the CEOP Command, United Kingdom National Crime Agency, United Kingdom, and Daniel Kardefelt Winthers of the UNICEF Innocenti Research Centre, Florence, Italy, for giving direction and sharing the benefits of their experience at different stages of the process, as well as the participants in the Global Kids Online research who shared their experiences generously in March 2016.

At UNICEF Delhi we would like to thank Joachim Theis (Chief, Child Protection), for guiding the entire process, and Tannistha Datta (Child Protection Specialist), Serena Tommasino (Child Protection Specialist) and Ruchira Gujral (Corporate Partnership Specialist).

UNICEF would like to thank the lead authors, Neelam Singh and Karuna Bishnoi, for undertaking this assessment of child online abuse in India, as well as Sushobhan Mukherjee for his contributions.

Contents

Acronyms and abbreviations

BRICS	Brazil, Russian Federation, India, China and South Africa
CBI	Central Bureau of Investigation
CCVC	Centre for Cyber Victim Counselling
CEOP	Child Exploitation and Online Protection Centre (United Kingdom)
CERT-In	Indian Computer Emergency Response Team
CSAM	Child sexual abuse material
DEITY	Department of Electronics and Information Technology
DNS	Domain name system
DoT	Department of Telecommunications
DSCI	Data Security Council of India
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes
FBI	Federal Bureau of Investigation (United States)
FIR	First Information Report
IAMAI	Internet and Mobile Association of India
IC4	India Cyber Crime Coordination Centre
ICMEC	International Centre for Missing and Exploited Children
ICT	Information and communication technologies
ISIL	Islamic State in Iraq and the Levant
ISP	Internet service provider
IPC	Indian Penal Code
IPS	Indian Police Service
IT	Information technology
IWF	Internet Watch Foundation
LLF	Learning Links Foundation
MLAT	Mutual legal assistance treaty
MMS	Multimedia messaging service
NCRB	National Crime Records Bureau

NCMEC	National Centre for Missing and Exploited Children [United States]
NCPCR	National Commission for the Protection of Child Rights
NGO	Non-governmental organization
NLSIU	National Law School of India University
NPC	National Policy for Children
NSSO	National Sample Survey Organization
PC	Personal computer
SMS	Short message service
SOP	Standard operating procedure
TRAI	Telecom Regulatory Authority of India
URL	Uniform resource locator
VoIP	Voice over Internet Protocol

Glossary[1]

Term	Definition
Child pornography[2]	"Any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose."[3]
Child sexual abuse	Forcing, luring or persuading a child by any older person, male or female, to take part in sexual activities, which may happen with or without physical contact, offline or online. (The new Terminology Guidelines clarify that sexual abuse of children requires no element of exchange, and can occur for the mere purpose of the sexual gratification of the person committing the act. Such abuse can be committed without explicit force…The mere fact of the sexual activity taking place is sufficient to constitute abuse. Furthermore, child sexual abuse can take the form of both contact and non-contact abuse.)
Child sexual abuse material	Sexually explicit representation of children. (The new Terminology Guidelines define this as material depicting acts of sexual abuse and/or focusing on the genitalia of the child.)
Child sex tourism	Deliberately seeking out children for sex during travels while taking advantage of the sense of anonymity afforded by the opportunity. (Under the new Terminology Guidelines, this term should be avoided and can be replaced by the term "sexual exploitation of children in the context of travel and tourism".)
Commercial sexual exploitation of children	A form of sexual exploitation (of children) where the focus is specifically on monetary benefit through activities like production and consumption of child sexual abuse material ("child pornography"), prostitution of children, abuse and exploitation in the travel and tourism industries ("child sex tourism") and trafficking in children for purposes of sexual exploitation. (The new Terminology Guidelines state simply that "a distinction can … be made between 'sexual exploitation' and 'commercial sexual exploitation', with the latter being a form of sexual exploitation where the focus is specifically on monetary benefit, often relating to organized criminality where the primary driver is economic gain".)

[1] This report was drafted prior to the issuance of the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse adopted by the Inter-agency Working Group in Luxembourg on 28 January 2016. As a result, not all of the terminology used in this report is in alignment with the new guidelines.

[2] The terms "child sexual abuse material" is now preferred over "child pornography" to dispel the notion of willingness on the part of the child in any way and to reflect the grave nature of the content.

[3] The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

Term	Definition
Cyber defamation	Using words or images or signals online to lower the reputation or prestige of the target.
Cyber extremism	Any measure of imposing predetermined ideology using any online or digital platform, beyond the norms of existing common social way of life[4]
Cyber harassment	Messaging abusive or other objectionable content to the target child or creating fake profiles in social media with the intention of targeting him or her.
Cyber intimidation	Communicating direct or implied threats through emails or messages in social media to inspire fear in the target child.
Cyber stalking	Following someone on Internet/mobile for causing inconvenience, or harassment/extortion, or for other illegal motives.
Digital literacy	The ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.[5]
Digital media	Digitized content (text, graphics, audio, and video) that can be transmitted over Internet or computer networks.[6]
Exposure	Public display, posting or forwarding of personal and private communication, images or video of the target child.
Feature phone	Low-end mobile phones with embedded limited third-party software for control, monitoring and data manipulation.[7]
Grooming	Preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation. (The new Terminology Guidelines define grooming as "the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person".)
Malware	Specifically designed "malicious software" (such as spyware to key loggers, computer viruses and worms or Trojan horses) that damage or disrupt computer operations, or gain access to gather sensitive information private computer systems, or display unwanted advertising.

[4] <http://www.urbandictionary.com/define.php?term=Cyber%20Extremism>

[5] <http://connect.ala.org/node/181197>

[6] <www.businessdictionary.com/definition/digital-media.html>

[7] <www.gsmarena.com/glossary.php3?term=feature-phone>

Term	Definition
Online sexual harassment	Unwelcome sexual advances, request or demand for sexual favour, and other verbal or physical conduct of a sexual nature. "Sexual harassment" refers not only to sexual conduct with the explicit intention to violate the dignity of another person (i.e. purpose) but also to conduct of a sexual nature that a person experiences as offensive or intimidating
Pharming	Installation of malicious code on a personal computer or server, misdirecting users to fake or fraudulent websites without their knowledge or consent.
Phishing	The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information. The user is usually directed to a website and asked to update personal information (e.g. password, credit card, bank account numbers) that is misused for identity theft.[8]
Prostitution of children	"The use of children in sexual activities for remuneration or any other form of consideration." The optional protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Article 2(b) (The new Terminology Guidelines recommend this term should not be used, and that "exploitation of children in prostitution" should be used instead.
Sexting	Self-production and posting of intimate pictures, sexually explicit conversations, posting/sharing of intimate pictures.
Smart phone	A cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system, web browsing and the ability to run software applications. Currently, the two major smartphone platforms in use are Android (by Google) and iOS (by Apple). An application written for a specific platform can usually work on any smartphone using the same platform. Applications for smartphones are faster and better integrated with the phone's user interface than Java applications.[9]
Social exclusion	Using online platforms to message the target child that he or she is not included with the peer group and its social activities.

[8] <www.webopedia.com/TERM/P/phishing.html>

[9] <www.gsmarena.com/glossary.php3?term=smartphone>

Term	Definition
Social media	The collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.[10] Facebook, Twitter, Google+, Wikipedia, LinkedIn and Pinterest are some of the social media platforms popular in India.
VoIP caller ID (Voice over Internet Protocol caller identification)	A caller ID application for VoIP phones that works in much the same way as caller ID on a conventional telephone line but with enhanced features and flexibility.[11]
Trafficking in persons	"The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation."

[10] <whatis.techtarget.com/definition/social-media>

[11] <http://searchunifiedcommunications.techtarget.com/definition/VoIP-caller-ID>

Executive summary

This report was commissioned by UNICEF to gain an overview of child online safety in India. The report aims to provide a useful source of information for child protection actors, law enforcement agencies, information and communication technology (ICT) companies, government ministries and anybody concerned about children's online safety.

1. Access to information and communication technologies in India

There are currently about 400 million Internet users in India. While India's rate of Internet access is still relatively low compared to that of other middle-income countries, it is quickly catching up. Most of the growth in Internet access is driven by mobile Internet use.

Major disparities exist in Internet access due to socioeconomic differences, geographic coverage and gender. While 60 per cent of urban dwellers have access to the Internet, only 15 per cent are online in rural areas. The digital divide is equally stark between men and women. In urban areas, women make up one third of Internet users, whereas in rural areas only 10 per cent of Internet users are female. Virtually all urban middle-class men of working age now have Internet access through smartphones, although almost all poor rural women are offline. Many poorer and rural users continue to use basic feature phones for communication and entertainment. The patterns of Internet use also vary between rural and urban areas, with urban users increasingly going online for communication, social networking, shopping and ticketing and rural users still predominantly for entertainment. Little reliable information is available on children's access to the Internet. While less than 10 per cent of schools in Bihar, Assam and Jharkhand have personal computers (PCs), virtually all schools in Kerala and Chandigarh have PCs.

2. Online risks and threats for children in India

Digital technologies offer significant developmental and educational benefits for children. However, the growing access and use of ICT by children also increases their exposure to potential risks of online abuse and exploitation. Cyber offences against children are spreading and diversifying as new methods are used to harass, abuse and exploit children. In many instances, children are also online offenders. Digital technologies provide new avenues to reinforce and spread existing social and cultural norms, as well as to mediate virtual social contexts and relationships. Offline forms of crime and violence against children are finding new forms of expression in the online world and their effects on children are amplified. In many cases offline and online violence are interrelated, with online abuse also including offline components. Non-contact abuse can be harmful to children and can facilitate the transition to contact abuse. Being able to stay anonymous online and impersonate others may embolden people into offensive and criminal acts and lower the deterrent potential of laws.

Current forms of child online abuse and exploitation include:

- **Cyberbullying:** emotional harassment, defamation and social exposure, intimidation, social exclusion
- **Online sexual abuse:** distribution of sexually explicit and violent content, sexual harassment
- **Online sexual exploitation:** production, distribution and use of child sexual abuse material (CSAM) (child pornography), "sextortion", "revenge pornography"
- **Cyber extremism:** ideological indoctrination and recruitment, threats of extreme violence
- **Online commercial fraud:** identity theft, phishing, hacking, financial fraud
- **Habit formation and online enticement to illegal behaviours:** access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure
- **Grooming:** preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation

There are no reliable figures on the extent, patterns and trends of child online abuse and exploitation in India, since no comprehensive surveys have been carried out on these issues. Several ICT companies have conducted surveys and polls among urban youth. These surveys focus mostly on young people's use of the Internet and do not provide more in-depth data regarding online risks. National crime statistics include a category of cybercrime, but this focuses only on commercial fraud and online radicalization, with no component of child online abuse. Although there are several sources of data on child online sexual exploitation, including Childline, law enforcement and ICT companies, these sources have not been analysed and access is often restricted due to privacy concerns and the reluctance of ICT companies to be associated with child sexual abuse.

3. Child online protection response system

The multidimensional and fast-changing nature of ICT and social media poses unprecedented challenges for the prevention of and response to child online abuse and exploitation. In order to establish child online protection systems, adequate structures, coordination mechanisms, capacities and resources need to be established. One of the key challenges is the transnational nature of the Internet. Conventional legislative frameworks and law enforcement are ineffective in the face of crimes and offences committed in the virtual world by people who live in other countries or continents.

a) Monitoring, reporting and removing online child sexual abuse material

In order to ensure prompt removal of CSAM, effective collaboration is needed between the ICT industry and law enforcement agencies. India does not yet have a hotline for reporting and removing online CSAM. Data on the reporting and removal of CSAM is not monitored and few people in India have the skills and knowledge to report CSAM. Adequate guidance, protocols or coordinated response are lacking.

The following actors have responsibilities for monitoring and removing CSAM in India:

- The National Technical Research Organization is responsible for infrastructure for internal and external security with the Intelligence Bureau monitoring cases of terrorism and insurgency but not child abuse cases. The Computer Emergency Response Team (CERT-In) is the national nodal agency responsible for issuing instructions to block websites.
- CSAM is reported to the police Cybercrime Cell which seeks clearance from the Department of Telecommunications and from the Department of Electronics (DoT) and Information Technology (DEITY) to block sites containing illegal content.
- The Central Bureau of Investigation (CBI) has a key role in the engagement with INTERPOL for keeping tabs on websites spreading child pornography. INTERPOL maintains a "worst of" list which has details of such websites that can be used by authorities in India. Any request to block websites has to come through DEITY and not directly from CBI.
- The Indian Cyber Crime Coordination Centre (IC4) was set up to coordinate with different agencies to prevent and minimize damage from cyberattacks. IC4 has direct access to the Crime and Criminal Tracking Network and Systems and the National Intelligence Grid – India's two largest crime databases.
- Mumbai-based Aarambh is collaborating with the United Kingdom-based Internet Watch Foundation (IWF) to establish a national hotline for reporting, removal and blocking of CSAM.
- Social networking and messaging platforms and search engines such as WhatsApp, Facebook, Twitter, Instagram, Flickr, MySpace and Google block and report offensive and abusive material via filters, privacy settings and complaint mechanisms. Since 2011, social media platforms have been using the Photo DNA technology developed by Microsoft to scan every uploaded photo to control the distribution of CSAM. Search engines such as Google and Bing also block the search of illegal material and use splash pages to warn users when they are about to access illegal or harmful content.
- To stop the sharing of illegal online material, collaborative mechanisms have been established between global Internet companies and law enforcement agencies such as the National Center for Missing and Exploited Children (United States), Child Exploitation and Online Protection Centre (CEOP) (United Kingdom), Internet Watch Foundation (IWF) (United Kingdom), INTERPOL and the Federal Bureau of Investigation (FBI) (United States).

b) Criminal investigation and prosecution of online sexual abuse and exploitation

Cybercrime investigation is the domain of the police. However, few cases of cyber offences involving children as victims or offenders are reported to the police and even fewer reach the courts. There have been few convictions for child online abuse and exploitation in India. Law enforcement suffers from a range of shortcomings that hamper effective investigation of child online abuse:

- Inadequate knowledge of cyber laws and **limited enforcement capacities** undermine reporting and investigation of cases. The training of law enforcement officers has not been upgraded to respond to the ever-evolving complexity of cyber offences.
- **Cybercrime cells and cyber forensic capacities:** India currently has 23 cybercrime cells. The Data Security Council of India (DSCI) has developed standard operating procedures and a manual for cybercrime investigation. Cyber forensic laboratories are attached to some cybercrime cells for computer, network and mobile forensics and for training on cybercrime and cyber forensics.

Conviction rates for child online abuse are extremely low; specialized skills, capacity and resources are needed from key actors, and especially law enforcement, to appropriately handle cyber evidence in cases of child sexual abuse. Infrastructure and technological deficits prevent cyber forensic labs from processing large volumes of evidence. There is a need for notified labs and to build specialist capacities in cyber forensics. Industry associations such as DSCI (established by NASSCOM)[12] have helped to strengthen cyber forensic investigation capacities. The cybercrime investigation programme of the Police Modernization Scheme is helping with the establishment of cybercrime police stations and cybercrime investigations and forensic training facilities in all states and union territories.

Police training: The CBI Training Academy has set up a cyber forensics training lab to train CBI officers in cyber forensics and investigations and the National Police Academy conducts training courses on cybercrime and forensics for Indian Police Service officers. CERT-In and the Centre for Development of Advanced Computing train law enforcement agencies, forensic labs and the judiciary in collecting, analysing and presenting digital evidence.

Judicial processes: There are no special or fast-track courts for cyber offences and the justice system is already overloaded. While 605 special courts have been set up under the Protection of Children from Sexual Offenses Act, 2012 there is little confidence in the capacity of these courts to handle child sexual abuse cases.

International cooperation is the key to tackling challenges of jurisdiction in the online environment. Indian authorities are able to obtaining support from Indian Internet service providers (ISPs), but face major challenges in getting cooperation in accordance with Indian laws from global social media platforms, search engines and ISPs, most of which are under United States jurisdiction.

c) Identification, reporting and services for child victims of online exploitation and abuse

In principle, child online offences can be reported directly to the police or via Childline. In practice, lack of understanding of cyber offences by front-line police officers discourages

[12] National Association of Software and Services Companies, a national trade association for India with over 1,850 companies registered. www.nasscom.in

victims from doing so. In 2015, Childline noted a significant increase in the reporting of child online abuse cases and is facing challenges in providing adequate responses to child victims.

Under-reporting of child online abuse: Online offences against children are generally underreported due to a lack of awareness of the law and limited understanding of what constitutes abuse or exploitation. The National Crime Records Bureau (NCRB) only monitors reported cases, which do not reflect the actual incidence of cyber offences against children.

Data collection and analysis: Weak recording systems limit the quality of data analysis. Annual NCRB reports do not collate information on cybercrimes against children. By 2016, the Crime and Criminal Tracking and Network System is expected to record all cases registered at police stations.

Services for victims of child online exploitation and abuse: Only a few facilities exist for child victims of cyber offences and they have limited outreach and are of uneven quality. Specialized facilities for counselling and rehabilitation tend to be concentrated in urban areas. The juvenile justice administration lacks counselling services for underage online offenders and there is no standard response protocol for cases of online abuse and exploitation within the education system. Capacity development initiatives for functionaries of the Integrated Child Protection Scheme do not yet include the management of online abuse and exploitation cases. Training modules are due to be revised in 2016 to include cyber safety. Initiatives by a few non-governmental organizations (NGOs) such as Tulir and Aarambh respond to the needs of victims of child online exploitation and abuse.

4. Prevention through education for digital literacy and safety

One of the key gaps identified in this assessment is the general lack of understanding of professionals, policymakers and society as a whole of the risks and threats posed to children by ICT and social media. No single agency can ensure the safety of children from online abuse and exploitation. Relevant government institutions, the private sector, international organizations, academia and civil society have to work together to build structures, mechanisms and capacities to prevent and respond to child online abuse and exploitation. A safe online ecosystem for children requires technical solutions and a high degree of preparedness, collaboration and coordination among stakeholders. A number of initiatives raise awareness of online risks.

Role of Government: DEITY, part of the Ministry of Communications and Information Technology, has launched a five-year project on information security, education and awareness. This programme promotes awareness of information security among children, families and professionals.

The ICT sector has a key role to play to prevent and respond to child online abuse and exploitation. DSCI, a body set up by NASSCOM, has conducted social awareness campaigns to educate children and adult Internet users about cybersecurity and cybercrimes. The Internet and Mobile Association of India has supported a school and college outreach programme on safe web surfing and digital wellness. Intel Security's Cybermum champions online safety for children through Intel's security portal, Twitter and Facebook. Telenor's Webwise introduces first-time users to the Internet's potential for information and learning and to online risks of bullying, abuse and malware. As part of India's Digital Literacy and Internet Safety Campaign, Google's Web Rangers programme empowers teens to promote safe Internet use among children. Microsoft released the "Stand Up To Online Bullying" quiz and "Digital Citizenship in Action" toolkit and educates adults to talk with children about online safety.

Few **civil society organizations** have addressed child online protection issues due to a lack of technological know-how. Tulir Centre for the Prevention and Healing of Child Sexual Abuse is raising public awareness of child sexual abuse and prevention and support services for child victims. Bachpan Bachao Andolan's 2015 Full Stop campaign raised awareness of cyberbullying, cyberstalking and sexting. Freedom from Abuse of Children from Technology, a programme launched by the Asian School of Cyber Laws, informs parents and children about online threats and how to mitigate them. These NGO initiatives tend to have limited reach and do not adequately address the growing need for informed and responsible use of the Internet.

Partnerships between the ICT industry and civil society: A number of digital safety education and awareness programmes have been initiated by ICT companies and service providers in collaboration with civil society organizations. Facebook has worked with NGOs on online safety programmes for adolescents and parents. Google and Facebook have supported Learning Links Foundation, which works with education professionals and policymakers to improve online education systems. The Twitter for Good initiative addresses issues related to freedom of expression, women in technology, emergency crisis response, improving access and inclusion and digital citizenship.

5. Legislation and policies to protect children online

a) Existing policies and laws

India's policy and legal framework for cybersecurity is evolving and, despite its limitations, provides a base for building a comprehensive strategy for child online protection. The following laws exist to address cybercrimes:

- The **Information Technology Act, 2000,** which addresses aspects related to cyberspace, and the Information Technology (Amendment) Act, 2008 are the main pieces of legislation concerned with online activities and cover any communication device used to transmit any text, video, audio or image. The provisions of the National Cyber Security Policy, 2013 enable the development of a dynamic legal framework.

- The **National Policy for Children** (NPC), 2013 does not refer directly to online risks. All policies related to education, ICT or cybersecurity are expected to incorporate the principles of the NPC and provide children with equal opportunities for learning and empowerment, while protecting them from harm.
- The **National Policy of ICT in Schools,** 2012 is more explicit about regulating ICT to protect children from potential risks. It recognizes online risks and has provisions for regulating and monitoring Internet access. The promotion of ICT systems in schools and adult education is included in the National Education Policy.
- The **National Cyber Security Policy,** 2013 addresses the prevention, investigation and prosecution of cybercrimes, including those against children. It calls for strengthening capacities of law enforcement agencies to investigate cybercrimes and gather data to enable prosecution.
- The **Indecent Representation of Women (Prohibition) Act,** 1986 prohibits indecent representations of women and criminalizes the performance of obscene acts and songs but does not punish the audience or those who make the person perform such acts.
- The provisions of the Information Technology Act have been strengthened by the **Protection of Children from Sexual Offences** Act, 2012 which deals with online offences against children, including child pornography and grooming. As the Information Technology Act does not have specific provisions for criminal intimidation, hate speech and defamatory content, the provisions of the Indian Penal Code apply in cases of online offences.

b) Limitations of policies and laws

The effectiveness of these legal provisions is undermined by the lack of clear definitions coming from cultural perceptions of right and wrong, what is acceptable and unacceptable and obscenity and decency, and by inequitable gender relations.

Lack of a uniform terminology: A universal terminology of online abuse and exploitation of children is imperative for clear and effective communication on the issue as well as the interpretation and application of laws and policies. Disagreements regarding the meaning of terms have created confusion for policy, legislation, interventions and public advocacy. Legal instruments defining and criminalizing sexual exploitation of children have not kept pace with new forms of sexual exploitation of children through ICT. Some key legal instruments predate technological advances. For example, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography does not criminalize live-streaming of child sexual abuse or online sexual grooming. The Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, adopted by the Interagency Working Group in Luxembourg on 28 January 2016 and published in June 2016, are an important step that will support the harmonization of language used in legal instruments and communication tools to protect children in the online environment.

Lacunae in the law: Many activities that have been criminalized in other countries, such as sexting and cyberbullying, are not regarded as offences by Indian law. Legal provisions for addressing cyberbullying are lacking. While child trafficking with the intent of sexual exploitation is criminalized, child trafficking with the intent to produce pornography and advertise child sex tourism online is not. Establishing the criminality of grooming and sexting is difficult and probably not desirable in view of the potential for misuse of the law. Children and adults have to be educated to exercise caution as grooming can be the pathway to potential harm, and sexting and self-exposure can enhance children's vulnerability.

Subjective interpretation of legal provisions: In the absence of clear law enforcement guidelines, there is considerable scope for conflicting interpretations of legal provisions pertaining to the online safety of children.

Balancing protection and privacy: Children's right to privacy is pitted against their right to protection. Protection often requires proactive measures, including surveillance, which tends to intrude upon children's right to privacy.

Children accused of cyber offences: There is a need to develop approaches that do not criminalize children and adolescents for harmful online behaviours.

6. Recommendations for priority interventions

The following recommendations were developed during the expert consultation on child online safety held in Delhi in April 2016.

Leadership and partnerships for child online safety in India

- Identify key organizations and potential partnerships to lead, coordinate and monitor inter-agency efforts to ensure appropriate prevention and response to child online exploitation and abuse.
- Develop a National Framework for Child Online Safety and a multi-agency action plan to be implemented through multi-sectoral partnerships and collaboration; including clear definitions of roles and responsibilities.
- Build awareness and capacity of key partners including ICT companies, government bodies, law enforcement agencies, media, civil society actors, etc.

Evidence, research and data on child online safety in India

- Carry out a study of the risky and harmful online behaviours of children in and out of school.
- Carry out a study of the production, distribution and use of CSAM based on data available from law enforcement agencies, ICT companies, Childline and media reports.

Education for digital literacy, citizenship and safety

- Bring together key education actors to agree on a common action plan on digital literacy and safety.
- Develop a plan to institutionalize and mainstream digital safety and literacy to reach a very large proportion of children, caregivers and relevant professionals.
- Develop an age-appropriate curriculum on digital safety, literacy and citizenship to be integrated and mainstreamed in the school curriculum across subjects, particularly as part of the ICT curriculum.
- Ensure active and meaningful engagement of children and adolescents in protecting themselves and their peers from online abuse and exploitation.
- Enable and empower parents and caregivers to play an active role in preventing and protecting children from child online abuse and exploitation.

Legislation and policies to protect children from online abuse and exploitation

- Review and revise cyber laws related to child online abuse and exploitation.
- Invest in the implementation of cyber laws and legislations via improved child-centred guidelines, structures, capacities and resources.
- Develop approaches that do not criminalize children and adolescents for harmful online behaviours.

Reporting and removing online child sexual abuse material

- Invest long-term in an India-based hotline able to remove high volumes of CSAM.
- Establish and reinforce collaboration between the ICT industry and law enforcement actors to ensure effective reporting and removal of online CSAM.
- Raise awareness of mechanisms for the reporting and removal of CSAM among children, parents and professionals.
- Monitor, analyse and review data on the reporting and removal of CSAM.

Legal investigation and prosecution of online child sexual abuse and exploitation

- Invest in the capacities and resources of the police workforce and cyber forensic professionals.
- Clarify and strengthen processes and procedures for cybercrime investigations.
- Improve coordination and collaboration between cybercrime cells, police and the ICT industry.
- Apply a child-centred approach to CSAM reporting and to the legal investigation and prosecution of child online abuse and exploitation.

Services for victims of the worst forms of child online abuse and exploitation

- Integrate child online protection in processes to strengthen child protection systems and define a specific intervention package for holistic support for victims of child online abuse.
- Map the responsibilities and skills required by child protection system actors.
- Develop a programme to strengthen capacities for child online protection across the child protection system.
- Develop capacities for online counselling of children victims of online abuse and exploitation (e.g., Childline).

Introduction

In recent years, India has seen a rapid spread in the use of smartphones and the Internet. Digital India and other policy initiatives of the Government of India, along with the interest of multinational companies in harnessing the potential of the Indian market, are fostering the expansion of information and communication technologies (ICT) at a pace and scale never witnessed before. According to the latest Mobile Internet in India report, there were 306 million mobile Internet users as of December 2015. Of these, 219 million users are from urban India and 87 million from rural India. There was a remarkable growth of 77 per cent from December 2014 and the mobile Internet user base is projected to reach 371 million by June 2016.[13] Mobile Internet penetration in India is 23 per cent as of December 2015, with online chatting (76 per cent) and social networking (73 per cent) the leading activities performed by mobile Internet users in 2015.

The rapid development and expansion of ICT have generated new opportunities for the realization of children's rights as well as significant challenges for the protection of children from abuse and violence. ICT and particularly social media offer children and adolescents new means to enhance knowledge, skills and participation as well as new

[13] Internet and Mobile Association of India (IAMAI), *Mobile Internet in India*, New Delhi, 2015.

spaces to engage in play, socialization and entertainment. However, the lack of digital literacy and online safety measures expose children to high risks of online crime and abuse such as cyberbullying, harmful material, grooming and sexual exploitation.

Media reports and a growing body of research indicate an emerging phenomenon of children and young people as both victims and offenders in online or ICT-mediated violence in India. The magnitude of online or ICT-related crimes and abuses towards children in India remains unknown and there are no coordinated preventive and response mechanisms in place. Some studies have been carried out focusing on child online protection in India and a number of non-governmental organizations (NGOs), government departments and experts are working on the issue. However, significant gaps remain in terms of knowledge, reporting mechanisms, response services, law enforcement and preventive strategies to respond to and prevent child online abuse, violence and exploitation.

It important to note the significance of the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, adopted by the Interagency Working Group in Luxembourg on 28 January 2016. The guidelines were published in June 2016, after the assessment was conducted and this report prepared. As far as possible, we have made every effort to update the definitions used in this report, and going forward the new Terminology Guidelines will be an important tool for everyone working to protect children from exploitation and abuse, both online and offline.

There is an urgent need for data gathering, coordinated action, evidence-based policies, legislation and interventions to establish a safe online environment for children. In order to respond to this need, UNICEF commissioned this assessment of the child online protection context in India to provide UNICEF and its partners with a comprehensive overview of the child online safety ecosystem and its gaps and opportunities in India.

Purpose

The purpose of this assessment is to map and review existing legislation, structures and mechanisms to protect children from online violence and to identify key stakeholders and services for child victims of online exploitation and abuse. Based on this gap analysis and in consultation with key experts, this report outlines a number of promising practices and priority interventions to improve the online safety of children and adolescents in India.

Methodology

The assessment was funded by WeProtect Global Alliance—End Child Sexual Exploitation Online, a global initiative to prevent and tackle child sexual exploitation. The study was guided by the framework developed by UNICEF headquarters to research, plan and programme for child online safety. The assessment included a comprehensive review of available documents, semi-structured interviews with key informants and expert consultations.

Literature review: A comprehensive list of resources was drawn up through recommendations and Internet searches. A range of international guidelines and publications, India-specific reports and grey literature were reviewed. Data from recent surveys about the manifestations of child online abuse in India were reviewed with reference to the methodology, sample size and consistency of findings.

Semi-structured interviews were conducted with subject specialists, representatives of government ministries and departments, NGOs and representatives from the corporate sector to further investigate child online safety. Relevant individuals, organizations and institutions provided information and insights into the legal, technical and social dimensions of the child online context in India.

Expert consultations: A workshop was held with representatives of ICT companies on 8 February 2016 to discuss the guidelines developed by the International Telecommunication Union and UNICEF to strengthen collaboration for promoting online safety of children. Following the circulation of the draft assessment report, a consultation was held on 8–9 April 2016 with a select group of experts to explore opportunities for strengthening child online safety in India and to articulate priority recommendations and agree on key follow-up actions.

Limitations

The assessment had a number of limitations. The absence of an accepted terminology for offline and online risks, abuse and exploitation of children posed significant challenges to the assessment process. Also, the fast-changing nature and terminology related to ICT and social media posed a challenge throughout the review and consultation process. The Luxembourg Guidelines cover the online dimensions of violence against children and will provide much needed terminological clarity.[14]

While efforts were made to review all available literature and documentation on the subject, there are still gaps. Gathering timely and high-quality data on ICT, social media and child protection remains a challenge. Existing studies on children's use of the Internet are of variable quality, use small sample sizes, often do not publish their methodology and are usually not comparable across different surveys. The types of surveys carried out by ICT companies also are not suitable to research the worst forms of online violence and exploitation of children. Law enforcement agencies have information about the online sexual exploitation of children, but these data have not been published in India.

Child online risks and abuse have been largely associated and limited to child pornography in India with the result of narrowing the scope of public dialogue on the issue. Furthermore, conservatism within Indian society has hindered an open discussion on issues that are associated with sex and sexuality, especially when children and young

[14] The new global terminology guidelines (known as the "Luxembourg Guidelines") were published in June 2016. The Interagency Working Group is composed of the Special Representative of the Secretary-General on Violence against Children, the United Nations Special Rapporteur on Sale of Children, Child Prostitution and Child Pornography, ECPAT International and 13 other international organizations and agencies active in the field of children's rights. See <www.ecpat.net/news/interagency-working-group-adopts-global-terminology-guidelines-sexual-exploitation-and-sexual>

people are involved. Embarrassment, disdain or possible consequences of the discussion on such a topic may restrain some of the informants from sharing information and opinions.

The aim of the assessment was to provide UNICEF and its partners with a comprehensive overview of the child online safety ecosystem and its gaps. Efforts to gather data about the manifestations of child online abuse and exploitation and to obtain information from children were deliberately moved to the next phase of UNICEF child online safety work in India. Moving straight into research with children, without first having a clear understanding of the wider child online ecosystem, would have risked not only asking the wrong questions, but also of gathering data without understanding how it could be used for programming and policy advocacy. The assessment also highlighted that two separate studies with different methodologies would be required, one on children's own use of ICT and another more specifically on the online sexual exploitation of children.

The authors made every effort to reach out to key stakeholders for inputs, comments and feedback. Further clarifications were obtained on the draft versions to validate the findings and conclusions of the report. The report is not intended to provide an exhaustive review of the entire child online protection realm in India but rather to provide an overview of emerging patterns, initiatives and potential high impact interventions. It aims to focus on some key aspects of the child online protection ecosystem in India that were identified as particularly important by the stakeholders in terms of learning and moving forward with collective actions to better protect children in India.

Audience

This report aims to reach all stakeholders involved in the various aspects of preventing and responding to the online abuse and exploitation of children. This includes ICT companies, law enforcement agencies and law makers, government and non-governmental child protection agencies, as well as educators and the media responsible for raising awareness and educating people about the benefits and risks of digital technologies.

Structure of the report

The first section of the report takes stock of the expansion of ICT and the online environment in India. This is followed by a discussion on the manifestations of online violence, abuse and exploitation of children in India. The third section outlines the emerging child online protection system in India including existing relevant structures, mechanisms and capacities. The fourth section focuses on preventive approaches via education for digital literacy, skills and safety of key stakeholders across India. The fifth chapter provides an overview of the current status and limitation of the legislative framework addressing child online abuse and exploitation in India. The final section outlines the way forward, including a set of priority recommendations.

1 Expansion of ICT and social media in India

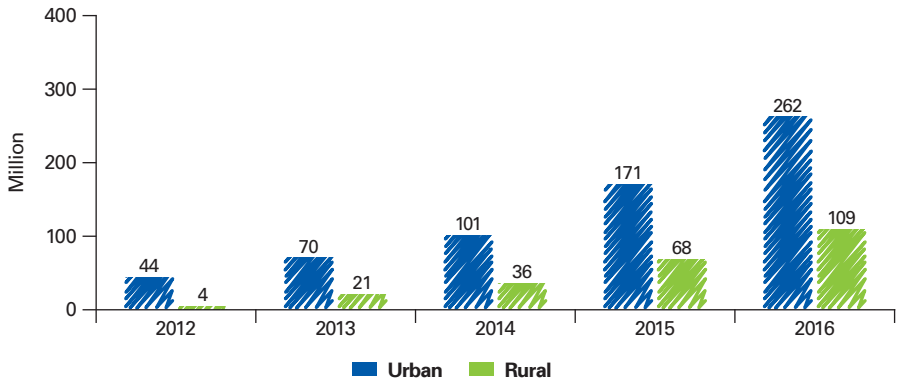
India is quickly catching up with the rest of the world in the adoption and integration of digital technologies in everyday life. India is one of the most dynamic ICT markets in the world and is the largest sourcing destination for the information technology (IT) industry, counting an IT workforce of about 10 million people and hosting the innovation centres of several global IT firms. Moreover, Indians have shown exceptional interest in adopting ICT, particularly mobile phones, spurred by their growing affordability and the convenience they offer in many spheres of life. The ongoing evolution and rapid adoption of ICT and social media, whether devices, services or processes, are affecting Indian society as a whole, including children's lives. Taking stock of the current ICT expansion in India is important to set the basis for an improved understanding of the digital environment in which Indian children and adolescents exist and interact, and experience its benefits as well as risks and threats.

This chapter provides a brief overview of the current ICT landscape and digital context in which Indian children and adolescents learn, engage and interact.

1.1 Mobile-led expansion of the Internet

India has the second largest mobile phone subscriber base in the world, as a result of affordable smartphones and mobile Internet packages. The ubiquitous mobile phone is one of the symbols of the changing landscape of India as subscriptions have boomed in recent years and cost-cutting by telecom providers has lowered prices and led to some of the cheapest tariffs in the world. According to the Telecom Regulatory Authority of India (TRAI), India's mobile phone subscriber base reached more than 1billion users in 2015, making it the only country after China to achieve this milestone.[15] Indeed, mobile phone subscriptions outnumber landlines, which are showing diminishing popularity.[16]

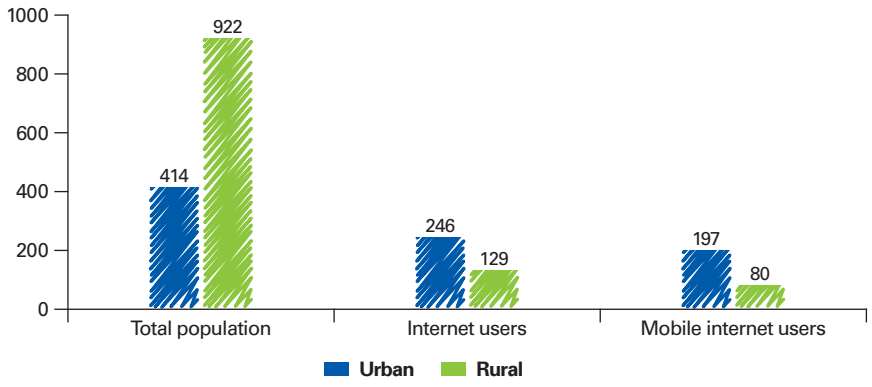
Graph1: Mobile internet users in India



Data source: IAMAI & IMRI, 2015

A defining feature of the Indian ICT market is the overwhelming use of prepaid mobiles, with the vast majority of consumers opting for a pay-as-you-go model. The share of smartphones in the overall mobile phone market was around 40 per cent in 2015. Current trends indicate that smartphone sales will overtake feature phone sales in 2016. This constitutes a significant shift for Internet consumption. Three fourths of Indians access the Internet on their mobiles. For many, a mobile phone represents their sole means of accessing the Internet, leading smartphones to overtake desktop computers as the most popular way to go online.

Graph 2: Internet users in 2015 (in million)



Data source: IMRB & IAMAI, 2015

[15] TRAI, 'Highlights of Telecom Subscription Data' as on 31 January, 2016, Press Release No. 22/2016, New Delhi, March 2016.

[16] Ibid.

It took more than a decade for India to move from 10 million to 100 million Internet users, three years from 100 million to 200 million users and just one additional year to reach 300 million users.[17] In addition to the increased availability of affordable smartphones, the expansion of spaces with free Wi-Fi could pave the way for a surge in Internet usage. Smartphone shipments to India grew 29 per cent in 2015 to reach 104 million and may increase at double-digit rates in 2016. At least one in two smartphones shipped in India in 2016 is expected to be a 4G enabled device.[18]

Box 1: Digital India

Recognizing the potential of ICT and social media, the Government of India launched Digital India as a national flagship programme with a vision to transform India into a digitally empowered society and knowledge economy. Digital India's vision includes the following elements:

Digital infrastructure as a utility for every citizen

- High-speed Internet as a core utility
- "Cradle to grave" digital identity -unique, lifelong, online, authenticable
- Mobile phones and bank accounts enabling participation in the digital and financial space
- Easy access to common service centres
- Shareable private space on a public cloud
- Safe and secure cyberspace

Governance and services on demand

- Seamlessly integrated across departments or jurisdictions
- Services available in real time from online and mobile platforms
- All citizen entitlements available in the cloud
- Services digitally transformed for improving ease of doing business
- Making financial transactions electronic and cashless
- Leveraging Geospatial Information Systems (GIS) for decision support systems and development

Digital empowerment of citizens

- Universal digital literacy
- Universally accessible digital resources
- All documents and certificates available in the cloud
- Digital resources and services in Indian languages
- Collaborative digital platforms for participative governance
- Portability of all entitlements in the cloud[19]

[17] IAMAI, *Internet Readiness Index in India*, New Delhi, February 2016.

[18] International Data Corporation (IDC) *Asia/Pacific Quarterly Mobile Tracker*. Cited in 'Samsung widens market share in India, remains No1 smartphone vendor: IDC', 17 February 2016. <www.livemint.com/Consumer/jZCn6LceSNfuXAFj4vKhuL/Samsung-widens-market-share-in-India-remains-No1-smartphone.html>

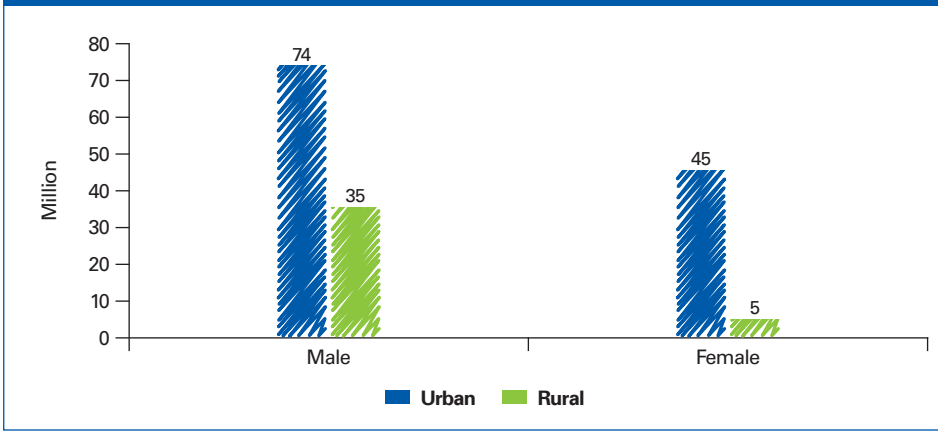
[19] Digital India national flagship programme of the Government of India. <www.digitalindia.gov.in/content/about-programme>

India represents the largest untapped consumer pool for global ICT companies and they seem willing to offer low-cost Internet to reach more than 1 billion people, including many English speakers. ICT companies also offer their services in Indian languages. Facebook's Free Basics programme, essentially a differential pricing programme for a limited basket of Internet services, has been banned in India, with regulators affirming commitment to net neutrality.

1.2 The digital divide

Despite India having the second largest mobile phone subscriber base in the world, access to ICT and the Internet is highly unbalanced across the country. Pervasive digital divides between states and union territories, urban and rural areas, socioeconomic classes and genders are reflected in inequitable ownership and use of devices, in differential rates of Internet adoption, in points of access and in the type of services and information accessed.

Graph 3: Internet users by gender and location (October 2014)



Many people in urban areas have more than one connection, while teledensity in socioeconomically disadvantaged states and union territories as well as in remote rural areas is far below the national average.

Only 7 per cent of rural Indians have Internet access, compared to 76 per cent of urban people. According to the National Sample Survey Organization (NSSO), in 2014 just 6 per cent of households in villages and 29 per cent of households in cities owned a computer. Only 27 per cent of households with at least one member aged 14 years or above had Internet access (16 per cent among rural and 49 per cent among urban households). Low teledensity in parts of the country may adversely impact improvements in living standards and access to services. For instance, improved Internet access is a precondition for the success of the national e-governance initiative, Digital India. In order to fully realize the potential of the ICT sector, existing infrastructure deficits and last-mile connectivity need to be addressed.

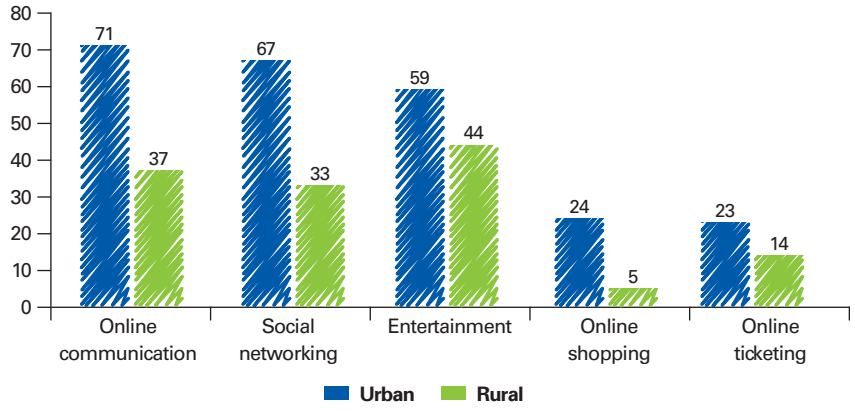
In terms of interstate differences, a recent index of "Internet readiness" places Maharashtra, followed by Karnataka, Gujarat, Telangana and Tamil Nadu, at the top of the list of Indian states in terms of mobile and Internet infrastructure, e-participation or use of online transactions and services by citizens, status of the IT service sector and

available e-governance services.[20] The NSSO, 2014 survey found that only about 4 per cent of households in Chhattisgarh and Bihar possessed computers compared to 31 per cent in Kerala. Chhattisgarh also had the lowest percentage (2.5 per cent) of rural households with Internet access, whereas in Kerala more than half of rural households had Internet access. In urban areas too, Chhattisgarh had the lowest rate of Internet access (25 per cent) compared to 62 per cent in Kerala and 65 per cent in Maharashtra.[21] The NSSO 2014 survey found that three times more urban males (aged 14 years and above) were able to use computers for various purposes as compared to their rural counterparts.

The NSSO, 2014 survey found that three times more urban males (aged 14 years and above) were able to use computers for various purposes as compared to their rural counterparts

A recent study by the Centre for Communication and Development Studies explored barriers to Internet access for a broad spectrum of low-income and socially-excluded populations in Pune (an urban agglomeration in Maharashtra) where approximately 40 per cent of the population lives in informal settlements or slums. The research findings indicated that digital inequality reinforces existing social inequalities, and therefore constitutes a major social inclusion and public policy issue.[22] It identified the digitally deprived as mostly those who are also disadvantaged along the traditional axes of inequality. They include poor people without access to the infrastructure required to log on; those who lack education and necessary ICT skills; and those, especially women, who lack the freedom and autonomy to use digital technologies.

Graph 4: Purpose of internet use in India



Equally important is the fact that the Internet is still largely a male preserve in India. Only 29 per cent of Internet users are female. This proportion has remained unchanged over the past year, with 50 per cent growth in Internet usage among males compared with 46 per cent among females. The significant gender divide has implications for digital content and the tenor of the online discourse. Indeed, barely a quarter of Indian Facebook users are women and the proportion drops further as one goes from younger to older age groups.[23] In terms of ability to use computers, women in both rural and urban areas were

[20] IAMAI and Indicus Analytics, *Index of Internet Readiness of Indian States - 2015*, New Delhi, February 2016.

[21] NSSO, *Key Indicators of Social Consumption in India: Education*, 71st Round. NSS KI (71/25.2), New Delhi. January-June 2014.

[22] Srivastava A, et al., *Towards Digital Inclusion: Barriers to Internet Access for Economically- and Socially-Excluded Urban Communities*, Centre for Communication and Development Studies, Pune, 2015.

[23] IAMAI. *Internet in India*, 2015.

found to be lacking in comparison to their male counterparts.[24] Discrimination against girls and women in terms of access and utilization of digital technologies naturally leads to their exclusion from the benefits that technology offers, especially in terms of accessibility to information, services and opportunities.

In terms of Internet consumption, Indians are communicating and seeking information and entertainment, which reflects current global trends. There is a broad convergence in Internet usage between urban and rural India, with social networking, communication and entertainment as the top three activities. Among social and messaging platforms, Facebook and WhatsApp are the most popular in India. According to Connected Life, a study by global consultancy firm TNS, about 51 per cent of Indian Internet users log into Facebook daily for social networking and 56 per cent use Whatsapp for instant messaging.[25]

To date, millions of poor and rural people continue to use feature phones to access music, games and videos through top-up shops and Internet at cybercafes. However, growth rates of rural wireless telephone subscribers are expected to receive a boost from the rapid expansion in digital infrastructure. For instance, future growth is expected to be propelled by 3G (currently 2G) mobile communications technology and by 4G in urban areas (currently 3G). Moreover, a significant reduction in the average price of voice communication services has already narrowed the rural–urban divide in access to mobile phones. In recent years, India has achieved a high rate of mobile phone penetration through competition among ICT providers, while broadband services have not been able to keep pace.[26] However, broadband services have improved due to policy support, with an increase in the number of broadband subscribers from 99 million in March 2015 to 145 million in February 2016.[27] This is expected to facilitate the over-the-top services such as those enabling communication (e.g., Skype and Viber), social networking (e.g., Facebook, Twitter, and LinkedIn) and messaging (e.g., WhatsApp) over the Internet.[28] Also, between April 2015 and February 2016, the overall teledensity increased from 79 per cent to 83 per cent, and 103,643 km of pipes and 79,994 km of optical fibre cables were laid under the Bharat Net Project.[29]

The lack of ability and skills to effectively use ICT and the Internet also present huge challenges

The lack of ability and skills to effectively use ICT and the Internet also present huge challenges. An NSSO survey conducted in 2014 showed that only 18 per cent of those in the 14–29 year age group in villages and 49 per cent in cities were able to operate a computer. Furthermore, even those who were able to operate a computer lacked proficiency. Just 14 per cent of those aged 14 years and above who could operate a

[24] NSSO, *Key Indicators of Social Consumption in India: Education,* 71st Round. NSS KI (71/25.2), New Delhi. January-June 2014

[25] <http://www.livemint.com/industry/vU55FbKdIz9vIfkxUb0EoL/Facebook-tops-networking-WhatsApp-in-message-apps-in-India.html>

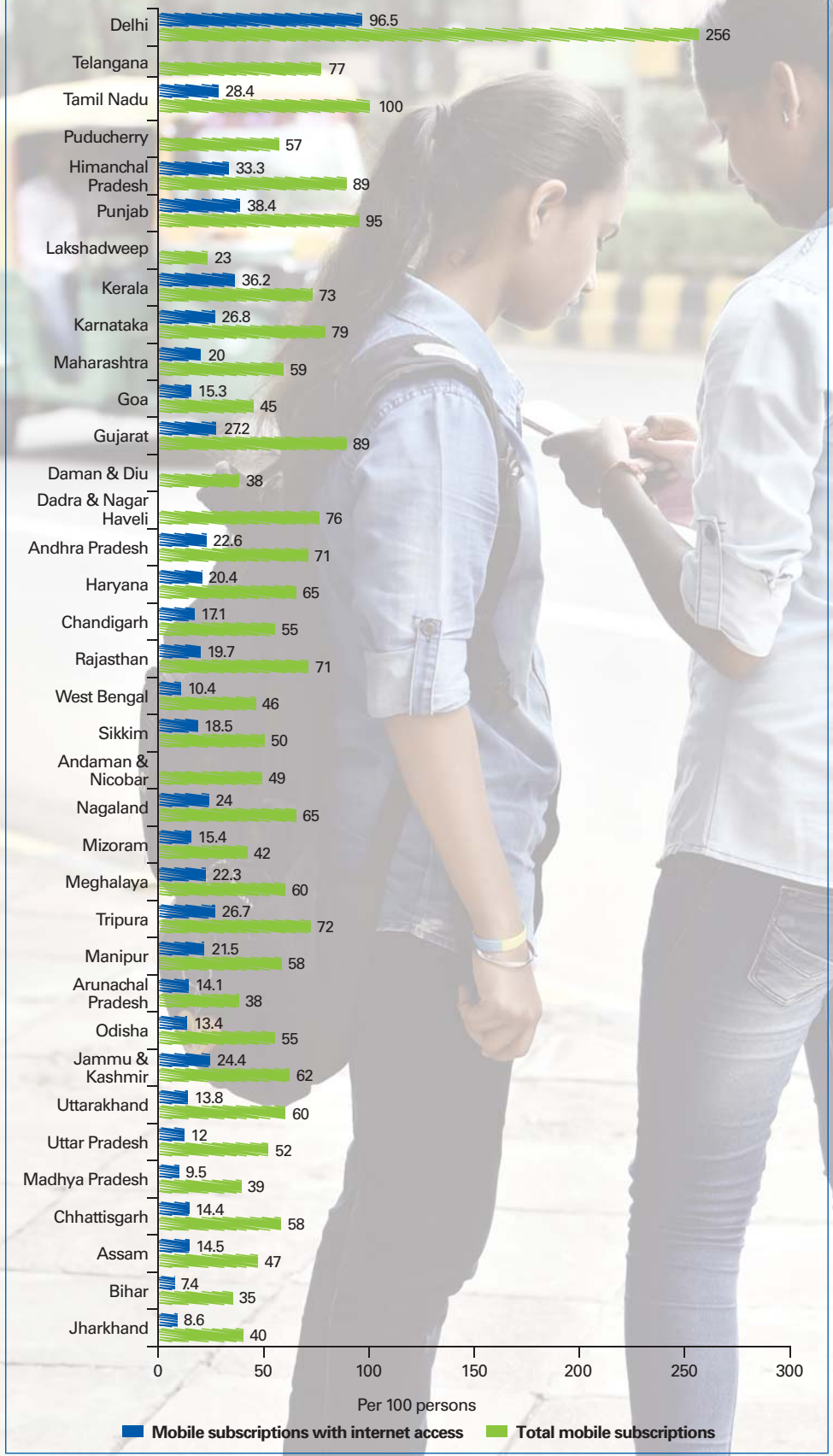
[26] Mani, Sunil and V Sridhar, 'Diffusion of Broadband Internet in India: Trends, Determinants and Challenges', *Economic and Political Weekly*, vol. I No. 51, December 2015. <www.epw.in/system/files/pdf/2015_50/51/Diffusion_of_Broadband_Internet_in_India_0.pdf>

[27] Telecommunications Regulatory Authority of India, 'Highlights of Telecom Subscription Data' as on 29 February 2016. <www.trai.gov.in/WriteReadData/PressRealease/Document/Press_Release_no26_eng.pdf> (2015a): The Indian Telecom Services Performance Indicators January–March 2015, Delhi.

[28] NSSO, *Key Indicators of Social Consumption in India: Education*, 71st Round. NSS KI (71/25.2), New Delhi. January-June 2014.

[29] <http://pib.nic.in/newsite/PrintRelease.aspx?relid=136863> and <www.trai.gov.in/WriteReadData/PressRealease/Document/Press_Release_no26_eng.pdf>

Graph 5: Mobile subscriptions in India



computer were able to type and use word processing.[30] The difference in digital literacy could be explained by different degrees of exposure to the Internet. One could argue that as people across India become more exposed to digital technologies, social networking, online shopping and e-governance, their digital literacy will expand and disparities in Internet use and proficiency are likely to shrink.

1.3 Children's use of ICT and social media

Although children and adolescents are often early adopters and drivers of ICT and social media, very little is known about their usage of digital technologies in India. Information and data on children's access and usage of mobile phones, Internet and social media are limited to a few studies. The patterns of availability, expansion and utilization are also constantly evolving.

There are only three main sources of data in India: the national Census, TRAI and the Internet and Mobile Association of India (IAMAI). The last Census was conducted in 2011, TRAI produces a report every quarter and the IAMAI releases its reports annually.[31] However, none of these sources provides a comprehensive and consistent picture of the situation in the country or provides information and data for children disaggregated by age and gender.

In terms of access to computers, one study shows that only one in four schools in India has a computer, irrespective of its functioning or access for children. Also, a large number of children in populous and socioeconomically disadvantaged states are not exposed to computers in their school (Graph 6). Generally, children who have access to computers at school live in urban centres and those who receive quality training and guidance are likely to attend better equipped and resourced private schools.

An IAMAI survey undertaken in 35 Indian cities indicated that about 28 million out of a total of 400 million Internet users were school-going children while a Telenor India study conducted in 2012 on child online safety in 12 countries found that children in India are in the highest risk category

In terms of children's Internet usage, the IAMAI survey undertaken in 35 Indian cities indicated that about 28 million out of a total of 400 million Internet users were school-going children.[32] Also, the proportion of children among rural Internet users has shown an increase from 5 per cent in 2014 to 11 per cent in 2015. It is worth noting that the majority of them are boys as per overall gender differentials indicated by the 2014 NSSO survey and studies by the Centre for Communication and Development Studies.

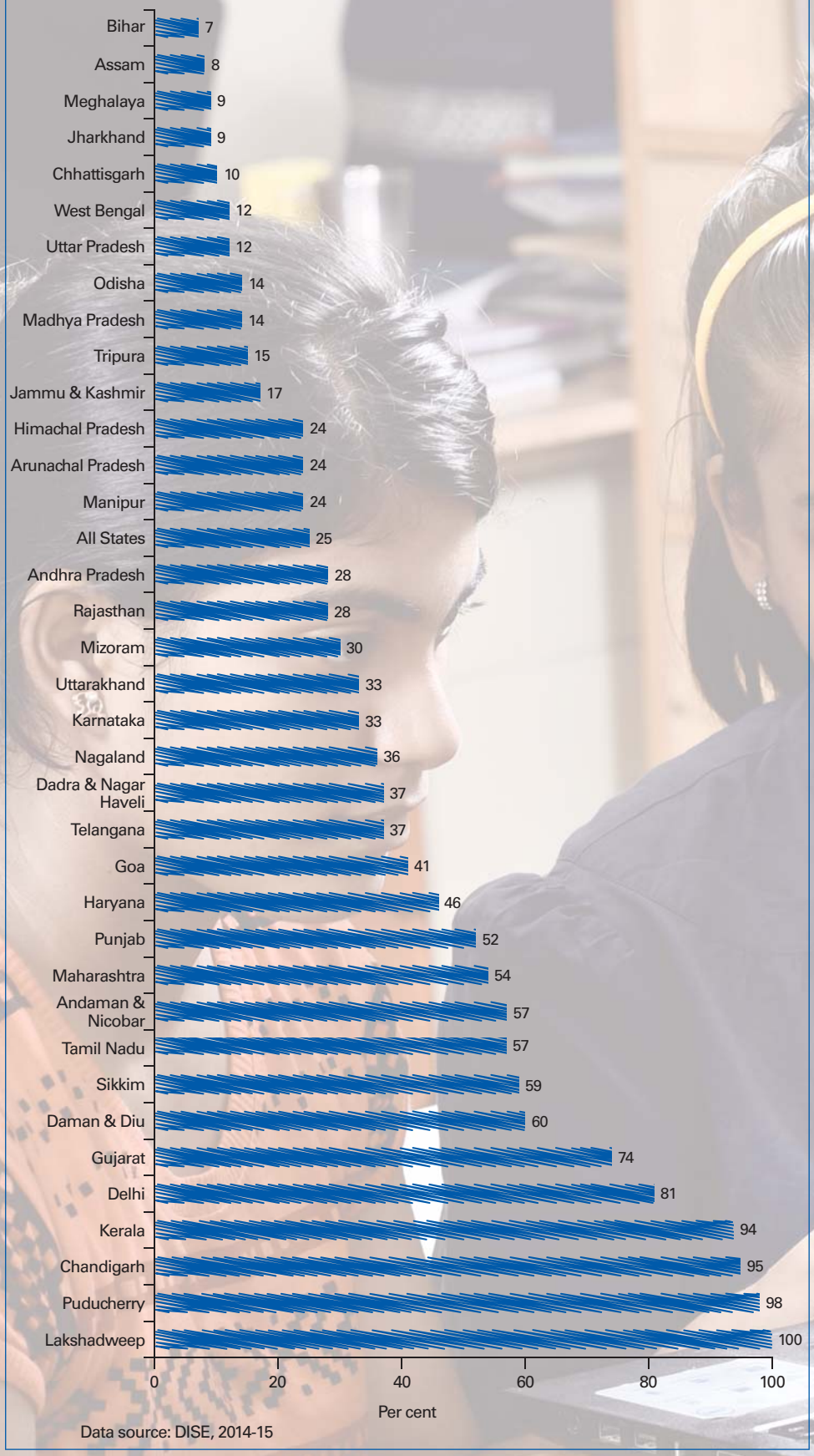
Survey findings are inconclusive regarding the extent to which Indian children are using the Internet for academic activities. Given the multidimensional accessibility and application of the Internet, it is debatable whether children use digital technology mostly for educational purposes or rather to chat with friends, listen to online music, watch videos or play online games while doing homework on a different website or app.

[30] Srivastava A, et al., *Towards Digital Inclusion: Barriers to Internet Access for Economically- and Socially-Excluded Urban Communities,* Centre for Communication and Development Studies, Pune, 2015

[31] <http://infochangeindia.org/digital-inequality/analysis/Internet-penetration-in-india-making-sense-of-the-numbers.html>

[32] IAMAI & IMRB, *Internet in India*, New Delhi, November 2015. <www.iamai.in/media/details/4486>

Graph 6: Schools having computers in Indian States/UTs



Data source: DISE, 2014-15

Children's digital literacy is an emerging challenge in India. In 2012, Telenor India did a study on child online safety in 12 countries and found that children in India are in the highest risk category due to a combination of increased access enabled by affordable Internet and smartphones, and low resilience with parents and children lacking the knowledge of how to safeguard themselves against different cyber threats.[33]

The adoption of digital technologies by children and adolescents has the potential to provide tangible benefits in terms of learning, access to information, socialization and active participation. However, the promises of digital technologies as instrumental to children's future success have to be tempered with the spectre of technology possibly acting as a force multiplier for offline threats and risks for children. These concerns are being experienced and expressed globally and in India.

The rapid adoption of digital technology is affecting societies at multiple levels and adding to the complexity of peer relationships, parenting and child protection. There is a need to strike a balance between allowing independent exploration and providing an appropriate level of oversight. Further understanding of how children and adolescents take advantage of opportunities offered by digital technologies across socioeconomic, age and gender divides in India is required in order to facilitate equal and safe opportunities for Indian children. Indeed, the protection of children from online risks and ensuring a safe Internet that will help children to develop their potential remains a key priority.

There is no empirical research and analysis on the patterns of online behaviour of boys and girls at different ages in rural, peri-urban and urban areas across India. Moreover, the public discourse on online abuse and exploitation in the country is very limited given the lack of knowledge and awareness of the risks and threats posed by ICT and social media to children. Child victims of online abuse and exploitation often lack the confidence and knowledge to report abuse and seek assistance. These factors pose significant challenges for advocacy, raising public awareness and education, as well as for the development of effective reporting mechanisms and services for child victims of online exploitation and abuse.

The public discourse on online abuse and exploitation in the country is very limited given the lack of knowledge and awareness of the risks and threats posed by ICT and social media to children

[33] Telenor & BCG, 2012. *Building Digital Resilience*. <www.telenor.com/morethan/wp-content/uploads/2016/05/Telenor-report-Building-Digital-Resilience.pdf>

2. Online risks and threats for children

While digital technologies offer significant developmental and educational benefits for children, the growing access to and use of ICT by children also increases their exposure to potential risks of online abuse and exploitation. In particular, the scope of cyber offences against children appears to be expanding as new and creative ways are identified and employed to harass, abuse and exploit them; in many instances, children are also the offenders.

Digital technologies provide new avenues to reinforce and spread existing social and cultural norms as well as to mediate new (virtual) social contexts and relationships. Hence, offline forms of crime and violence against children (e.g., bullying, discrimination, stalking, harassment, etc.) are finding new forums in the online world and their effects on the victims are amplified. In some cases "offline" and "online" violence are closely interrelated with online abuse also including offline components. For instance, non-contact abuse can be harmful to children and can facilitate the transition to contact abuse with wider ramifications. Moreover, the option to stay anonymous online, impersonate and cover tracks can embolden people into offensive and criminal acts and lower the deterrent potential of laws. These factors

In some cases "offline" and "online" violence are closely interrelated with online abuse also including offline components

pose significant and unique challenges to the protection of children and adolescents from online abuse and exploitation.

On one hand, online risks can be an extension of offline abuse with technology serving as a force multiplier. On the other hand, certain threats and risks are unique to cyberspace, such as those that involve the malicious and criminal use of ICT to harass and exploit children for sexual, discriminatory or commercial purposes. The intensity and reach of violence can be magnified by ICT with limited time for response and with existing child protection mechanisms being obsolete. For instance, if an inappropriate image or text about a child is shared on the Internet, it will remain public and not be easy to remove or retrieve.

Popular perceptions and literature tend to feed extreme views about the effects of opportunities and threats of ICT and the Internet for children and have the potential of undermining objectivity and balance in rapid situational assessments. Cases of child online abuse are hardly reported in the media or to the police in India and there is a complete lack of empirical research on online risks and threats for children. Neither academia nor the public sector has invested resources in ascertaining the prevalence or severity of the issue. The experiences of individuals and organizations working on this subject have not been sufficiently documented and analysed. The available research has been conducted by the ICT sector with objectives of knowledge dissemination and marketing. However, ICT companies and service providers generally are reluctant to share insights about users based about their confidentiality policies.

Cases of child online abuse are hardly reported in the media or to the police in India and there is a complete lack of empirical research on online risks and threats for children

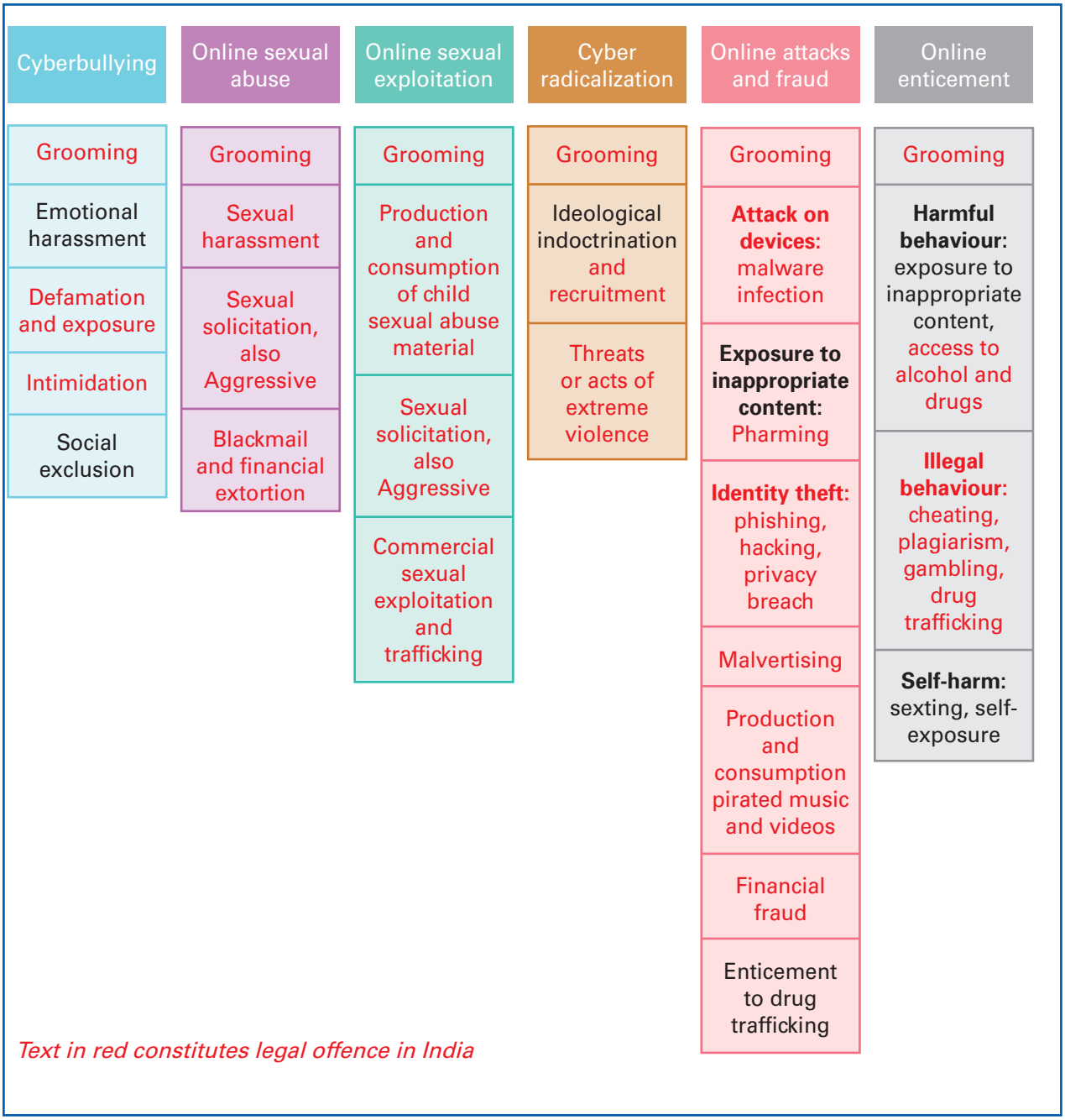
This chapter outlines the emerging manifestations of online risks and threats that children (and adults) may be exposed to in India (Figure 1)[34]. It is worth noting that the known manifestations involve various degrees of anonymity and familiarity and range from non-sexual to sexual and from inane to offensive. Legal offences according to the Indian legal framework are shown in red[35]. Legal offences may be difficult to establish due to systemic barriers and bottlenecks. Moreover, limited documentation and data and the fast changing and "virtual" nature of digital spaces pose significant barriers to the estimation of the extent to which children and adolescents in India are being affected.

It has to be kept in mind that online abuse cannot be seen and treated separately from offline abuse and exploitation. All forms of online abuse cause real harm to victims and most forms of online exploitation have links to offline abuse as well.

[34] Please refer to the glossary of this report for the definitions of the manifestations listed in Figure 1.

[35] It needs to be noted that a level of creativity is required to invoke and interpret available legal provisions in view of the inadequacy of the existing legal framework to respond directly to the evolving complexities of online offences.

Figure 1: Manifestations of child online threats, abuse and exploitation in India



2.1 Cyberbullying

Bullying among children is generally indicative of an imbalance of power or strength demonstrated through intentional or unintentional aggression repeated over time. It is known to involve hitting or punching (physical bullying); teasing or name calling (verbal bullying); intimidation through gestures or social exclusion (nonverbal bullying

or emotional bullying); and sending insulting messages by e-mail (cyberbullying).[36] Cyberbullying may involve "abuse and/or harassment by teasing or insulting, victims' body shape, intellect, family background, dress sense, mother tongue, place of origin, attitude, race, caste, class, name calling, using modern telecommunication networks such as mobile phones (SMS/MMS) and Internet (chat rooms, emails, notice boards and groups)".[37]

A study commissioned by Microsoft in 2012 ranked India third for high online bullying rates (after China and Singapore) among 25 countries where the survey was conducted. The study noted that half of the children aged 8–17 years in India who responded to the survey said that they had been subjected to a range of online activities that some may consider to be online bullying or to have adverse effects. About 22 per cent reported being subjected to mean or unfriendly treatment, 29 per cent had been made fun of or teased and 25 per cent had been called mean names.[38] The findings of recent research indicate similar or higher rates of cyberbullying in India with a significant number of children reporting having witnessed some acts of cyberbullying. The 2014 report of the Parliamentary Committee on Information Technology recognized that the online bullying of children by their peers was probably far more common than other offences.[39]

A study commissioned by Microsoft in 2012 ranked India third for high online bullying rates among 25 countries where the survey was conducted

Online and offline bullies display their power against another person by repeatedly manipulating the knowledge of the targeted child's context and sensitivities. While such hurtful online behaviour is unlikely to be considered as an offence under Indian law, the severity, frequency and pervasiveness of such messages can cause significant distress to the targeted child. The incidence of such exposure is bound to increase as mobile technology, images and videos become easier to access. The potent combination of anonymity, immediacy and reach in the case of cyberbullying adds to the challenge. While children tend to mirror adults' positive and negative behaviours, peers seem to play a critical role in influencing children's digital behaviour

The following are some of the emerging manifestations of cyberbullying in India.

Emotional harassment

As per the Teens, Tweens and Technology Survey commissioned by Intel Securities in India in 2015, 43 per cent of children active on social media claimed to have witnessed cruel behaviour on social networks, while 52 per cent of children indicated that they had themselves bullied people over social media. The main reasons for their behaviour cited by cyberbullies were that other children were mean to them (49 per cent) or they just did

[36] <www.cms.k12.nc.us/mediaroom/backtoschool/Documents/Bullying-Prevention%20Tips%20for%20Parents/Tips-Children%20Who%20Bullypdf.pdf>.

[37] Jaishankar, K., *Cyber Bullying: Profile and Policy Guidelines*. Tirunelveli: Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, 2009.

[38] Microsoft, *Global Youth Online Behaviour Survey*, 2012.

[39] Standing Committee on Information Technology (2013-14), Fifteenth Lok Sabha, Ministry of Communications and Information Technology, Department of Electronics and Information Technology, 'Cybercrime, cyber security and right to privacy', 52nd Report, New Delhi, February 2014.<http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf>

not like the other child (28 per cent). About 27 per cent made fun of others, 24 per cent called someone fat or ugly or made fun of other physical appearances, and 23 per cent tagged mean pictures.[40] Interestingly, more children owned up to bullying others than admitted that they had been victims themselves.

Defamation and exposure

The Internet has the potential to increase the potency of defamation as compared to conventional communication and media channels. Offensive content against a person is relayed much faster and to a much wider global audience through social media, e-mail groups, intranet, bulletin boards, chats, etc. The harm caused to a person by the online publication of defamatory statements about him or her can be greater than verbal and offline statements and can have vastly more damaging consequences. For children in particular, the effects of online communication of sensitive personal information, images or videos can be devastating and intimidating.

52 per cent of children indicated that they had themselves bullied people over social media

Intimidation

Online threats of stalking, violence, rape and death can be emotionally draining. Moreover, the effect of intimidation is further enhanced when the threatening message is shared with others and is followed by cyberstalking.

[40] <http://intelsecurityapac.com/digitalsafety/2015/10/27/research-india-ttt>

Social exclusion

Children and adolescents have a need for acceptance by their peers. Exposure of a child's private information or weaknesses exploits the developmental need of children to feel accepted and appreciated by their peers and feeds on their psychological insecurities. Being ridiculed, expelled from the peer group or discriminated against can have deeply harmful effects on a child. Of course, this is not unique to online social exclusion, particularly in the context of widespread caste-based discrimination.

Box 2: Examples of online offences committed by children in India

Since 2008, Rakshit Tandon, cybersecurity expert, has reached out to over 1.5 million students through a safe surfing programme. He currently supports cyber congresses in about 100 schools across India and receives approximately 30–40 requests for support from children and young people including cases involving "sexting".

A few examples of the cases he has dealt with:

- A 13-year-old boy was targeted by one of his classmates who used a fake identity to create a Facebook account to send out offensive messages to other children in the school. The victim did not have a Facebook account but was admonished by teachers and other parents.
- A girl was forced out of a school WhatsApp group where her morphed obscene picture was shared. The embarrassment caused to the girl was immense, although the school mediated in identifying and disciplining the offender.
- A girl in Class 9 sent over 30 sexually explicit photographs of herself through her mobile to a boy in Class 11. Taking the gesture as an invite from her, the boy sought a physical relationship but she was scared and backed out. The boy started blackmailing the girl, threatening to make her photographs public if she did not meet him. Finally, the girl and her friend approached the school counsellor who sought professional help and involved both sets of parents. The offensive photographs were removed; the boy confessed; and submitted a written apology.

2.2 Online sexual abuse of children

Child sexual abuse is defined as a sexual activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, for gratifying or satisfying the needs of the latter. Online child sexual abuse could be passive as in the case of exposing children to inappropriate online content or an active sexual solicitation.[41] Some of the most common forms of online sexual abuse of children in India are described below.

[41] *Sexual Harassment on the Internet.* <https://www.unc.edu/courses/2010spring/law/357c/001/internet harassment/internet-harassment.html>

Display of sexually explicit and violent content

Decades of research on the effects of exposing children to sexually explicit or violent pictures or videos have not resulted in conclusive findings. Some studies have shown negative effects, while others dispute these findings. The predominant sentiment among public officials in India is that children and adolescents should not be exposed to pornography. There have even been attempts to block pornographic sites in India. However, safeguards are often not in place and children may be

Due to the lack of safeguards, children may be exposed to sexually explicit and violent content on digital devices at home, in Internet cafes or through content easily uploaded to feature phones via memory cards

Box 3: The MMS case of an Adivasi girl in Birbhum

A 16-year-old tribal girl, who worked as a daily wage labourer to support her parents in Birbhum (West Bengal), was punished by the local *panchayat* for falling in love with a non-tribal boy from a nearby village in June 2010. She was stripped publicly, made to walk around the village for about two hours, sexually harassed by random villagers and photographed and videoed. These photographs and videos were sent as multi-media messages (MMS) to everyone in the village to ensure that no other village girl would dare to repeat her "crime".

No one, including the authorities at the nearby Mohammad Bazaar police station, came to her rescue and her shocked parents were of little assistance. She made her way back home only to be taunted by her neighbors and others. No case was registered against her attackers and no one defied the tribal *panchayat's* diktat. The evidence was tampered with, as community leaders were involved in the crime.

The girl spent a couple of months neglected and in isolation and then mustered the courage to lodge a complaint against those who had sexually harassed, violated and ostracized her. In doing so, she stood alone against the advice of her parents, family and friends. She reported the incident to the police and lodged a formal complaint, but there was no evidence except for the MMS. No one was willing to testify.

Two days after filing the complaint, the six main accused were arrested. Fearing a backlash from the community, the victim was sent to a government welfare home in Rampurhat. She continues to live there. Although she was honoured by the President of India with the National Bravery Award for standing up against the *panchayat*-like body, she leads a life of isolation and ostracism. She has not been able to go home as many members of her family refuse to speak to her.

Nonetheless, the district administration has arranged for her education, while women's organizations are demanding her rehabilitation in the community. The girl wants to finish her studies and fight for the rights of others who have been similarly abandoned.[42]

[42] *The Times of India*, 'Tribal teen stripped in Birbhum, molested by hundreds', Kolkata, 9 August 2010. <http://epaper.timesofindia.com/Repository/getFiles.asp?Style=OliveXLib:LowLevelEntityToPrint_TOI&Type=text/html&Locale=english-skin-custom&Path=TOIKM/2010/08/09&ID=Ar00101>

exposed to sexually explicit and violent content on digital devices at home, in Internet cafes or through content easily uploaded to feature phones (via memory cards) at top-up shops.

Sexual harassment

The motivation and frequency of action, lack of consent and sexual, defamatory or intimidating content define sexual harassment which involves sending undesirable content to a person and/or posting inappropriate content about him or her in cyberspace. A harasser who uses unwanted sexual attention to harass a victim online often intends to solicit sexual cooperation from his/her victim, either on the Internet or in person. The harasser may use personal communication to convey unwanted and unwelcome messages directly relating to sex and/or sexuality. Such messages often refer to intimate details of the victim's personal life and body, insinuate or offer sex-related activities or impose sex-related images or sounds.[43]

2.3 Online sexual exploitation

The precise number of child victims of online sexual exploitation in India or across the world is unknown. According to the International Association of Internet Hotlines, the number of webpages containing child sexual abuse material (CSAM) increased by 147 per cent from 2012 to 2014, with children 10 years old or younger portrayed in 80 per cent of these materials.[44]

Cyberspace provides fertile ground for children to be groomed, enticed and solicited into sexual activity for financial gains. In what is commonly termed as commercial sexual exploitation of children, someone other than the child usually benefits from a commercial transaction in which he or she is made available for sexual purposes. Images and videos of children and young people are also used for prolonged sexual exploitation through blackmail or sextortion.

The production and consumption of CSAM, or what is commonly termed as child pornography, is probably the most common form of online child sexual exploitation.[45] Although the production and distribution of pornography involving consenting adults is legal in many countries, producing and distributing photographs, magazines, books, drawings, movies, videotapes and computer disks or files with sexually explicit imagery of children is universally regarded as a crime. The report of the Parliamentary Committee on Information Technology in 2014 also recognized "the threat posed to children by predatory paedophiles, which conceal their true identity whilst using the Internet to 'groom' potential victims".[46] Nonetheless,

The number of webpages containing child sexual abuse material increased by 147 per cent from 2012 to 2014, with children 10 years old or younger portrayed in 80 per cent of these materials

[43] ibid.

[44] <www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx>

[45] The phrase "child sexual abuse material" is increasingly preferred to describe sexually explicit representation of children in place of the term "child pornography" as it dispels the notion of consent on the part of the child in any way and reflects the grave nature of the content.

[46] Jaishankar, K., *Cyber Bullying: Profile and Policy Guidelines*. Tirunelveli: Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, 2009.

special websites provide child sexual abuse materials for a cost (normally subscription) and some uncensored newsgroups charge a fee for membership and have child abuse images available as part of their service. Adults sexually abusing and exploiting children during travel (child sex tourism) are now using ICT and the Internet.[47]

There is an emerging global concern that child online sexual exploitation is likely to rise in the coming years with the demand for new CSAM. This new material includes the circulation of self-generated content, such as sexting and live-streaming child sexual abuse for which adults pay a fee to direct and view a live video of a child performing sexual acts in front of a webcam. Often young children are directed or sold by one of their parent to perform such sexual acts in front of the camera. Cases in which parents were paid a minimal fee (Rs. 500) to allow their child to be photographed or filmed with no clothes on or while performing sexual acts have been reported in some Indian states.

Messaging of sexually explicit content by way of images, photos, clips, video files or other material can increase the vulnerability of children and young people manifold. Many children participate willingly in conversations with subtle or explicit sexual undertones, and may not object to such messages either of their own volition or due to peer pressure. Many are also harassed, threatened or blackmailed into sending pictures. The growing number of reported cases of sexting and self-exposure highlight the vulnerability of children and young people to blackmail, extortion (including "sextortion") and "revenge porn". Criminals and predators are also believed to be capitalizing on the spread of the Internet and mobiles to sexually exploit children online through sexting, "sextortion" and grooming for sexual purposes through e-mail and voice over Internet protocol (VoIP).[48]

The growing number of reported cases of sexting and self-exposure highlight the vulnerability of children and young people to blackmail, extortion and revenge porn

[47] "Preferential" abusers deliberately seek out children for sex, and "situational" abusers take advantage of an opportunity during their travels.

[48] Halder D., and Jaishankar, K.,'Teen Sexting: A Critical Analysis on the Criminalization Vis-À-Vis Victimization Conundrums', *The Virtual Forum Against Cybercrime* (VFAC) Review, Korean Institute of Criminology, July–August 2014.

Box 4: Reported cases of blackmail and "sextortion"

Blackmail using videos of gang rapes in Fort Kochi

Six youths and two minors were arrested in January 2016 for alleged involvement in two different rape cases at a homestay in Fort Kochi in Kerala. The same person allegedly recorded the sexual assaults on his mobile phone to blackmail the victims in both incidents.

According to the police complaint, the gang rape took place two months earlier, when a youth and his friend had checked in at a homestay in Fort Kochi. A homestay employee called his five friends and locked out the youth, sexually assaulted his friend and recorded the act on a mobile phone. They took the girl's gold ornaments and fled in her friend's car, threatening to upload the video on social media if they dared approach the police. The youth was forced to pay Rs. 100,000 to get his car back. He decided to approach the Kochi police when he was threatened with the release of the video, if he did not pay Rs. 500,000.

After the sexual offenders were arrested, the police recovered images of another assault from the mobile phone. The other incident had taken place earlier in the month and also involved two minors.[49]

A shocking history of rape and blackmail in Hyderabad

The arrest of a college dropout in a blackmail and rape case in Bahadurpura in Hyderabad in March 2016 revealed shocking details of sexual exploitation, extortion and criminal intimidation of a teenage girl over a period of three years. The youth had shot some videos of intimate moments during a brief relationship with the victim's sister and used these to blackmail and rape the 17-year-old victim in 2012.

A college senior of the victim also blackmailed her about the "sexual relationship" she had with the college dropout and sexually exploited her for three months until she became pregnant. The girl was forced to have an abortion by the second accused in February 2014.

The first accused contacted the girl again on Facebook in September 2015 and resumed blackmailing her, claiming that he knew of her relationship with the second accused. He insisted that she should lodge a complaint against the second accused or else he would post her videos with the second accused on Facebook. He took her signatures on the complaint and also demanded Rs. 100,000. She paid Rs. 30,000 out of fear but also informed her parents who approached the police.[50]

[49] The India Express, Six youths arrested for 2 'rapes' at Fort Kochi', 25 January 2016. <http://indianexpress.com/article/india/india-news-india/six-youths-arrested-for-2-rapes-at-fort-kochi/#sthash.Faewe4ni.dpuf>

[50] Deccan Chronicle. 22 March 2016. <www.deccanchronicle.com/nation/crime/220316/hyderabad-arrest-reveals-shocking-history-of-rape-blackmail.html>

Sexting and self-exposure increase the vulnerability of children and young people to sexual abuse and exploitation and "revenge porn". People who work closely with children on child sexual abuse and exploitation and child online protection have observed widespread sexting and, to a lesser extent, self-exposure in the messages among both boys and girls, which essentially requires an exceptionally high level of awareness about the risks and consequences and astute personal judgment. Digital content once sent out is difficult to control and the consequences of an out-of-control sexting situation can range from trauma to criminal charges, reputation damage and, in some cases, even suicide. However, Indian cultural conservatism does not encourage open discussion about matters of sex and sexuality, which makes attempts to gauge the prevalence of sexting and self-exposure without invading privacy almost impossible.

Box 5: The Delhi MMS scandal of 2004

A sexually explicit MMS involving two 17-year-old students of a well-known school in New Delhi in 2004 remains a point of reference for cyber offences involving children. The actual act and the creation of the video using a mobile phone was reported for be consensual but its distribution and the bid to auction the clip on Baazee.com (now eBay India) were illegal. The two students were minors and were not prosecuted. The student who tried to sell the clip through the e-retail website got away because his possession of the clip could not be established and a sale had not been made. However, the CEO of the website was booked for allowing the listing of the clip.

This incident led to discussions on the efficacy of the Information Technology Act, 2000 and its Amendment, and in several instances led to a ban on mobile phones in schools and colleges. Even after a decade, many people, including informants for this assessment, referred to this case as a point of reference for cybercrimes involving children.

Children share explicit content using mobiles and the Internet for a variety of reasons. An overt expression of sexuality through talk and/or sharing of images is part of growing up as a boy in India. Girls, too, have had their own ways and means of dealing with their evolving sexual identity. Today technology offers boys and girls the means to express and explore, and even to go beyond stereotypical conduct and be what they want to be.[51]

Some children want to demonstrate their coming of age to their peers, either willingly or with a sense of discomfort, because everyone else is doing it. Some others want to fit in with their group of friends by boasting about sending or having photos on their mobile phones. However, empirical research is required to counter the tendency of people to generalize online behaviour, which could be detrimental for the agency, expression and participation of adolescent girls and boys.

Indian cultural conservatism does not encourage open discussion about matters of sex and sexuality, which makes attempts to gauge the prevalence of sexting and self-exposure without invading privacy almost impossible

[51] Interviews with Vidya Reddy, Director of Tulir (Chennai), New Delhi, 12 October 2015 and Rakshit Tandon, India cyber-security specialist, New Delhi, 20 November 2015

"Revenge porn" is the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress. The images are sometimes accompanied by personal information about the subject, including their full name, address and links to their social media profiles.[52]

Box 6: Revenge pornography

In April 2015, a 21-year-old man was booked by the police in the Nargol village of Valsad (Gujarat) for allegedly spreading photographs of his teenage ex-girlfriend in compromising positions on popular social media sites. The pictures were reportedly taken on a mobile phone but were posted by the accused when the girl's parents were reportedly looking for a groom for the girl. The accused was charged with molestation under different sections of the Information Technology Act and the Protection of Children from Sexual Offences Act.[53]

2.4 Cyber extremism

Cyber extremism is an emerging global problem with non-state actors increasingly using the Internet and social media to promote, propagate and implement radicalized thought processes, potentially threatening the security and integrity of nations.

Individuals living in remote areas are empowered by ICT and the Internet to access a wide range of information, including inflammatory content. While the free flow of information is the hallmark of a democratic society, inflammatory or radical information has the potential of aggravating a real or perceived sense of marginalization and persecution, inciting protests, violence and acts of terror by individuals and groups. Organized non-state actors are also known to be actively radicalizing children and young people in cyberspace.

The absence of international agreements on cyber extremism and the divergent national approaches to cyber law are also constrains to the establishment of cybersecurity at the global level.

The advent of cyber extremism has brought to the forefront relevant legal, policy and regulatory issues that need to be addressed through global cyber legal frameworks. The absence of international agreements on cyber extremism and the divergent national approaches to cyber law are also constraints to the establishment of cybersecurity at the global level. The risk of children and young people being indoctrinated and radicalized is increasing as a result of the serious threat terrorism poses to global security. Non-state actors may not have established a significant presence in India, but are known to have radicalized some youths.

[52] Be Aware B4 You Share. Revenge Porn, The Facts, <www.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf>

[53] *Times of India*, 'Are you a victim of revenge porn?', 19 April 2015. <http://timesofindia.indiatimes.com/life-style/relationships/man-woman/Are-you-a-victim-of-revenge-porn/articleshow/46852091.cms>

There is very limited information on the prevalence of cyber extremism India. In 2014, the British TV network, Channel 4, unmasked a Twitter handle – @ShamiWitness – widely known as one of the biggest propagators of the Islamic State in Iraq and the Levant (ISIL) on social media and revealed that it was operated by Mehdi Biswas, an Indian engineer working for a multinational corporation in Bengaluru.[54] ISIL has released India-specific material, including speeches and videos, in languages such as Bengali, Tamil and Malayalam in the past.[55] Although the number of Indians who have tried to join ISIL is believed to be negligible, many have been caught and display utter naivety based on the euphoric anti-Western propaganda of the group's online activities.[56]

2.5 Online commercial fraud

Cyber criminals have been finding new ways of employing the Internet to manipulate users and make illegal monetary gains. Financial fraud, production and consumption of

Box 7: Identity theft, hacking and breach of privacy

Phishing is the means to capture personal information by getting users to visit fake websites. Cybercriminals phish for bank account details and adopt numerous tactics to solicit e-mail address and password combinations from individuals. Typically, they lure an end-user to a web page designed to capture the user's e-mail account credentials. The compromised e-mail account is then used to attack more businesses and accounts by sending spam, phishing and malicious e-mails.

Pharming redirects unsuspecting users to a website determined by the hacker. Most domain name system (DNS) servers have security features to protect against such attacks but hackers are always on the lookout to test their immunity and find ways to gain access to them. Less common than phishing, pharming can affect many more people at once by modifying a large DNS server, resulting in the redirection of users to the wrong website.

Disrupting the attack in the early stages of the threat life cycle is critical. Recognizing the indications, taking necessary steps including antivirus programmes and contacting the ISP are important steps in dealing with the menace of pharming. Cyber safety experts envisage scaling-up of cybercrime with the growth in the use of mobile phones and the Android operating system. If previously there were 10–12 new malwares a month, now countless variations are coming out. Inadequate awareness and overconfidence in online security behaviour contribute to the vulnerability of consumers, especially children and young people.

[54] <www.channel4.com/news/isis-shami-witness-medhi-masroor-biswas-chargedhttp://www.channel4.com/news/isis-shami-witness-medhi-masroor-biswas-charged>

[55] <www.bbc.co.uk/newsbeat/article/31574846/how-islamic-state-extremists-use-social-media-to-recruit>

[56] ISIL is known to use the Internet for its media propaganda with great success, even leading to a lawsuit against Twitter ostensibly for being a tool for spreading extremist propaganda, fundraising and attracting new recruits. ISIL publishes a glossy magazine called Dabiq, releases well-produced theatrical propaganda videos, pays salaries to its jihadis and operates a quasi-state which advertises itself as a haven for the Islamist thought process.

pirated music, videos and films are now extensive online. As people spend more time on the Internet and engage in a growing variety of interactions, their exposure to online fraud increases proportionately.[57]

The exponential expansion of e-retail and the popularity of mobile phone-based apps in India, has created an ever growing number of teenage online shoppers who are vulnerable to online fraud. Indeed, sizeable numbers of online shoppers are based in aspirational semi-urban and better-connected rural areas. The TCS GenY surveys noted a drastic increase in the number of teenage online shoppers. The proportion of respondents who shopped online increased from 37 per cent in 2012–2013 to 68 per cent in 2013–2014. The surveys highlight that teenagers are now moving from buying low value items like movie tickets to purchasing high value items like designer clothes and accessories, with four in every 10 students buying clothes and accessories online.[58]

Most international research indicates that the time spent online has no direct impact on problematic outcomes or addiction while conceding that excessive use of mobiles and Internet may lead to tensions and conflict in the family

2.6 Habit formation and online enticement to illegal behaviours

A widely accepted perception in India is that continuous use of the Internet and games can be addictive in the long term, with effects ranging from attention deficiency to obsession and compulsion.[59] Empirical research on the impact of violent and/or sexually explicit audio-visual content is limited and conflicted. Most studies that show an effect (e.g., an increase in violent behaviour and desensitization after violent games) are experimental studies without an assurance of validity outside of the experimental condition. In addition, they show that the identified effects, if any, are not very long lasting. Most international research indicates that the time spent online has no direct impact on problematic outcomes or addiction while conceding that excessive use of mobiles and Internet may lead to tensions and conflict in the family.[60] In the absence of empirical evidence to support the claim that spending time online increases the risk of addiction, intragenerational conflict rather than mental disorder is cited as a possible cause for this perception.[61]

Experts define technology addiction as excessive use of mobile phones, Internet and social networking sites that lead to harmful consequences to a person's physical and mental health and social life. Although people can develop an addiction to these technologies irrespective of their age, this has been a growing concern among teenagers. It manifests itself in the form of obsessively checking the phone or accessing the Internet to see if there are any messages and the need to update their Facebook status, leading to social isolation, weight loss, poor personal hygiene, problems with eyesight and

[57] Several researchers have found that time spent online increased the likelihood of being a victim of a variety of cybercrimes, and the time spent online is being viewed as an important predictor with the increased probability of entering a dangerous website or using a dangerous service.

[58] <http://sites.tcs.com/genysurvey/>

[59] Interview with Dr. Tara, Internet Deaddiction Centre, Uday Foundation, New Delhi, 2 December 2015

[60] Kardefelt-Winther, D., 'A critical account of DSM-5 criteria for Internet gaming disorder', *Addiction Research & Theory - Early Online*, VOL. 23, Issue 2, 2014. And, Griffiths, M., et al., Working towards an international consensus on criteria for assessing Internet Gaming Disorder: A critical commentary on Petry et. al, Addiction, 111, 2014.

[61] Ibid.

backaches. Doctors feel this new-age affliction requires a clinical set-up to diagnose and suggest corrective measures, including professional counselling.

Box 8: Internet addiction: A reality or a myth?

In a recent case from India, two gaming-addicted brothers required a month of rehabilitation in the ward of the Ram Manohar Lohia Hospital in New Delhi. Several reports and articles in the media, which have been suggesting an increase in cases of Internet and gaming addiction, highlighted this case as an example of the perils of children spending excessive amounts of time on online gaming.[62]

Several Indian psychiatrists are reporting a spurt in cases involving addiction to gaming, social media and Internet surfing among children and young people, which disrupt their daily chores like washing, eating and studying.[63] This popular view also finds resonance in the findings of recent research by Action for Children in the United Kingdom that showed nearly a quarter of parents struggled to get their children to "unplug" and participate in activities away from television, phone and computer screens. When asked which behaviour they found most difficult to control in their children, more parents said they struggled to limit technology-based activity (23 per cent) than get children to eat healthily (19 per cent), go to bed (18 per cent) or do their homework (10 per cent).[64]

[62] *India Today*, 'So addicted to gaming, these kids urinated in their pants instead of going to the loo',19 February 2016. <http://indiatoday.intoday.in/technology/story/gaming-addiction-puts-youngsters-in-hospital/1/600202.html>. This specific case was reported prominently by most newspapers.

[63] *Hindustan Times*,'Reboot your brain: Phone addiction leads to depression', 10 October 2015. <www.hindustantimes.com/health-and-fitness/reboot-your-brain-phone-addiction-leads-to-depression/story-Rp2jHxPGz6zhsmCi5YIAFO.html; DNA India, Internet addiction killing personal touch,26 June 2012. <www.dnaindia.com/mumbai/report-Internet-addiction-killing-personal-touch-1706731>

[64] <www.actionforchildren.org.uk/news-and-opinion/latest-news/2016/january/unplugging-from-technology/>

Many children and young people are known to visit cybercafes to play competitive games like Defense of the Ancients (DOTA) 2, Counter Strike and Team Fortress but information on their interest and involvement in online gambling is less known. The Indian cricketer, Gautam Gambhir, highlighted the issue in his blog recently after he was informed by a school principal about children betting on Indian Premier League matches. Anita Pauline Dey, the principal of WH Smith Memorial School in Varanasi, found that children from Classes 6 to 10 in at least four states (names withheld) were indulging in betting on cricket matches. She discovered that most of these children were from affluent families and were using their pocket money and mobile phones to bet on matches through syndicates.[65]

While observers note that gaming appears to be an important area of interest among boys with Internet access, girls seem to be more engaged in the culture of "selfies"

While observers note that gaming appears to be an important area of interest among boys with Internet access, girls seem to be more engaged in the culture of "selfies". This may well be the situation or an exaggerated reflection of gendered behaviour in India. In either case, the subject needs to be explored with an appropriate and measured response. A Pew Research Center study in 2015 found that social media and online game playing were popular digital venues for meeting friends among children and young people; while

Box 9: The "selfie" phenomenon

Self-portrait photographs or "selfies" to be posted on social media using mobile phones and, if resources permit, the selfie stick, have become popular. There can be solo selfies, selfies with a partner and selfies in a group.[66] A Pew Research Center survey in 2014 placed the selfie craze in the domain of the young as 55 per cent of millennials reported sharing a selfie on a social site but only 33 per cent of the "silent generation" (those born between 1920 and 1945) even knew what a selfie was.[67] The popularity of selfies in India seems to buck this trend with the diffusion of mobile phones with cameras among older age groups and socioeconomically backward groups.

The increase in the number of cases of fatal accidents during selfie sessions are also a matter of concern. According to a report in the Washington Post, India suffered more selfie-related deaths in 2015 than anywhere else in the world. Approximately half of the world's 27 deaths linked to the pictures people took of themselves happened in India. Indeed, Mumbai police identified 15 sites around the city as "no selfie zones" after two people drowned in the Arabian Sea in January 2016, and announced plans to install warning signs and deploy lifeguards.[68]

[65] <www.kkr.in/gauti-speaks/24th-april-2016>

[66] <https://theconversation.com/why-do-people-risk-their-lives-or-the-lives-of-others-for-the-perfect-selfie-55937>

[67] Pew Research Center, *Millennials in Adulthood: Detached from Institutions, Networked with Friends*, March 2014. <www.pewsocialtrends.org/files/2014/03/2014-03-07_generations-report-version-for-web.pdf>

[68] *The Washington Post,* 'More people died taking selfies in India last year than anywhere else in the world', 14 January 2016. <www.washingtonpost.com/news/worldviews/wp/2016/01/14/more-people-die-taking-selfies-in-india-than-anywhere-else-in-the-world/>

boys are substantially more likely to meet new friends while playing games online (57 per cent vs. 13 per cent of girls), girls are more likely to meet them via social media (78 per cent vs. 52 per cent of boys).[69]

It is also possible for children and young people to buy illegal drugs online. Many companies sell drugs online in contravention of Indian laws, which do not permit sale or purchase of drugs on an e-commerce site.[70] They may also explore Darknet markets using Tor, the popular system for anonymous web browsing.[71]

As India evolves from an outsourcing hub for foreign gaming companies providing game development services and a limited user base of well-resourced urban consumers of console and personal computer (PC)-based games to a rapidly growing mobile phone-driven local market, the challenges are likely to be amplified. There is certainly a case for developing a substantive knowledge base on the psychological impacts of ICT on children in India. Systematic studies, including primary research, are needed to gauge the prevalence, dynamics and effects of addictive net surfing and gaming.[72] Although parental supervision and well-knit family systems are believed to be deterrents, there are sufficient pull factors for children to graduate from genuine interest into excessive use of ICT and social media. Imposition of legal limitations on sale or purchase, setting an age limit and restricting access to online games as deterrents are also options, but their efficacy needs to be investigated further.

[69] <www.pewInternet.org/files/2015/08/Teens-and-Friendships-FINAL2.pdf>

[70] Drug sales are regulated by the Drugs and Cosmetics Act, 1940, and the Drugs and Magic Remedies and Objectionable Advertisement Act, 1945. Under existing laws, only licensed retailers are allowed to sell drugs on the basis of a doctor's prescription. A license is mandatory even for over-the-counter drugs.

[71] <www.thrillist.com/vice/how-to-buy-illegal-drugs-online-with-the-darknet-tor-bitcoin-and-more-explained>

[72] Interview with Dr Achal Bhagat, Senior Psychiatrist, and Psychotherapist, New Delhi, 23 January 2016.

2.7 Grooming

Integral to enticing children into several abusive and exploitative situations, grooming entails luring a child into sexual conversations to prepare him or her for child sexual abuse and exploitation, or ideological or religious conversations to prepare him or her for violence and terror, or drugs and other illegal activities. It can take minutes, hours, days or months, depending on the goals and needs of the abuser and reactions of the child or young person.

Grooming entails luring a child into sexual conversations to prepare him or her for child sexual abuse and exploitation, or ideological or religious conversations to prepare him or her for violence and terror, or drugs and other illegal activities

Distinguishing grooming from conversations that result from increasingly intimate relationships or genuine enquiries and exchange of information and views based on shared interest is difficult. Forging friendships and courtship rituals do incorporate an element of grooming but the risk element is quite strong. In the event of ill intentions or a relationship gone sour, sexting and self-exposure can lead to harassment, blackmail, financial extortion and even sexual exploitation. Indeed, the possibility of technology being exploited in a society with

Box 10: Restrictions on the use of mobile phones by conservative community groups

Reports of caste- or religion-based social organizations (like Khap panchayats or caste councils of certain communities in Western Uttar Pradesh, Haryana and Rajasthan) issuing diktats on girls' way of dressing, communication and mobility are quite frequent and persistent in India. Such diktats hold the potential of widening gender disparities and digital use inequities.

- In 2015, a khap panchayat in Barmer in rural Rajasthan (Samdari panchayat in Barmer district of Kanana village and 12 kheda ke panchs of the Choudhary community) issued a diktat that girls of the village must not use mobile phones and social media and prohibited them from wearing jeans.[73]
- In 2015, a Muslim village panchayat banned mobile phones for unmarried girls in 10 villages in Muzaffarnagar and Saharanpur districts in Uttar Pradesh on the grounds that it results in increase of crimes and mischief.[74]
- In 2014, the panchayat of a Gujjar community in Jadwad village in Uttar Pradesh banned unmarried girls from wearing jeans and keeping mobile phones claiming that they were having a "bad" effect on them and were responsible for eve-teasing incidents.[75]

[73] *The Times of India*, 'Girls not to use mobile phones: Barmer Khap', 2 July 2015. <http://timesofindia.indiatimes.com/city/jaipur/Girls-not-to-use-mobile-phones-Barmer-khap/articleshow/47903726.cms>

[74] *DNA India*, 'Uttar Pradesh: Muslim village panchayat bans jeans, mobile phones for girls', 20 September 2015. <www.dnaindia.com/india/report-uttar-pradesh-muslim-village-panchayat-bans-jeans-mobile-phones-for-girls-2126940>

[75] *India Today*, 'Community panchayat bans jeans, mobile phones for girls in UP'. 10 August 2014. <Indiatoday.intoday.in/story/khap-community-panchayat-gujjar-girls-eve-teasing-jadwad-village-jeans-mobile-phones/1/376435.html>

extremely conservative sexual mores is high. Real or digitally altered nude images allow criminals to blackmail girls, and probably boys, for sex, money or both.

Halder and Jaishankar (2014) note that "Grooming and trapping children can be done by many ways, including simple chatting in the [most popular social networking sites]" and that "If the victim accepts the groomer as 'friend', it becomes easier for the groomer to acquire information about the maturity status of the victim. This is mainly acquired from the status messages that are shared by the victim, unclaimed pictures with messages embossed on them, which may be shared from other friends' collections, and so on. In case the child has an open profile, it becomes even easier for the perpetrator to trap him or her."[76]

Unlike in the West where online conversations precede offline sexual abuse and exploitation, the pattern in India appears to be the reverse. Online harassment, abuse and blackmail (including "revenge porn" and "sextortion") tend to follow offline harassment and relationships breaking down,[77] although cases of sexual predators lurking in cyberspace, forging friendships using fake identities, grooming and enticing children and young people to connect off-line are also known.

[76] Halder D., and K Jaishankar, 'Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites'; In C. Marcum and G. Higgins (Eds.), *Social Networking as a Criminal Enterprise* (pp. 129-143). Boca Raton, FL, USA: CRC Press, Taylor and Francis Group ISBN, 2014.

[77] Interview with Dr. Achal Bhagat, Senior Psychiatrist and Psychotherapist, 23 January 2016.

3. Child online protection response system

The multidimensional and fast-changing nature of ICT and social media, combined with problems related to regulation of the Internet, due to its transnational nature and the key role it plays in the democratization of information in society,[78] pose unprecedented challenges for the prevention of and response to child online violence. In order to establish and sustain child online protection systems and preventive strategies, adequate structures, coordination mechanisms, capacities and resources need to be operational. Traditional legislative frameworks are obsolete against the ubiquitous crimes and offences perpetrated in the virtual world. Indian legislation on child online protection needs to quickly adapt to technology developments and work in close collaboration with international law enforcement agencies and ICT companies to be effective. Strong multisectoral and international collaborations and coordination mechanisms are necessary to ensure that transborder child online abuse cases are investigated and prosecuted in a timely and effective manner.[79]

The Internet and social media can only be regulated and controlled to a certain extent as technological developments enable virtual offenders to swiftly find new ways to

[78] Halder D., & K Jaishankar, 'Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites'; In C. Marcum and G. Higgins (Eds.), *Social Networking as a Criminal Enterprise*, Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. ISBN, 2014.

[79] Interview with Karnika Seth, Cyber Law expert and visiting faculty to National Police Academy and National Judicial Academy, CBI Academy and National Investigation Agency, NOIDA 30 November 2015.

overcome control systems. It is also important to balance privacy with protection. The invasion of privacy poses a serious ethical and moral challenge to the task of preempting and proactively addressing online offences. Children's right to privacy often comes in conflict with the imperative of protection, and a shared narrative on the boundaries has not emerged in India.[78] Prepaid mobile phones present another barrier to monitoring or regulating Internet access for children. They are convenient for consumers but create major challenges for law and order organizations as well as service providers attempting to track errant behaviours and help bring offenders to justice. Finally, because cases of online offences against children are rarely reported, there is no indicator of the actual incidence and prevalence of child online abuse and exploitation in India. All of the above pose incredible challenges to ensuring the online safety of Indian children and require innovative and technologically advanced approaches and solutions.

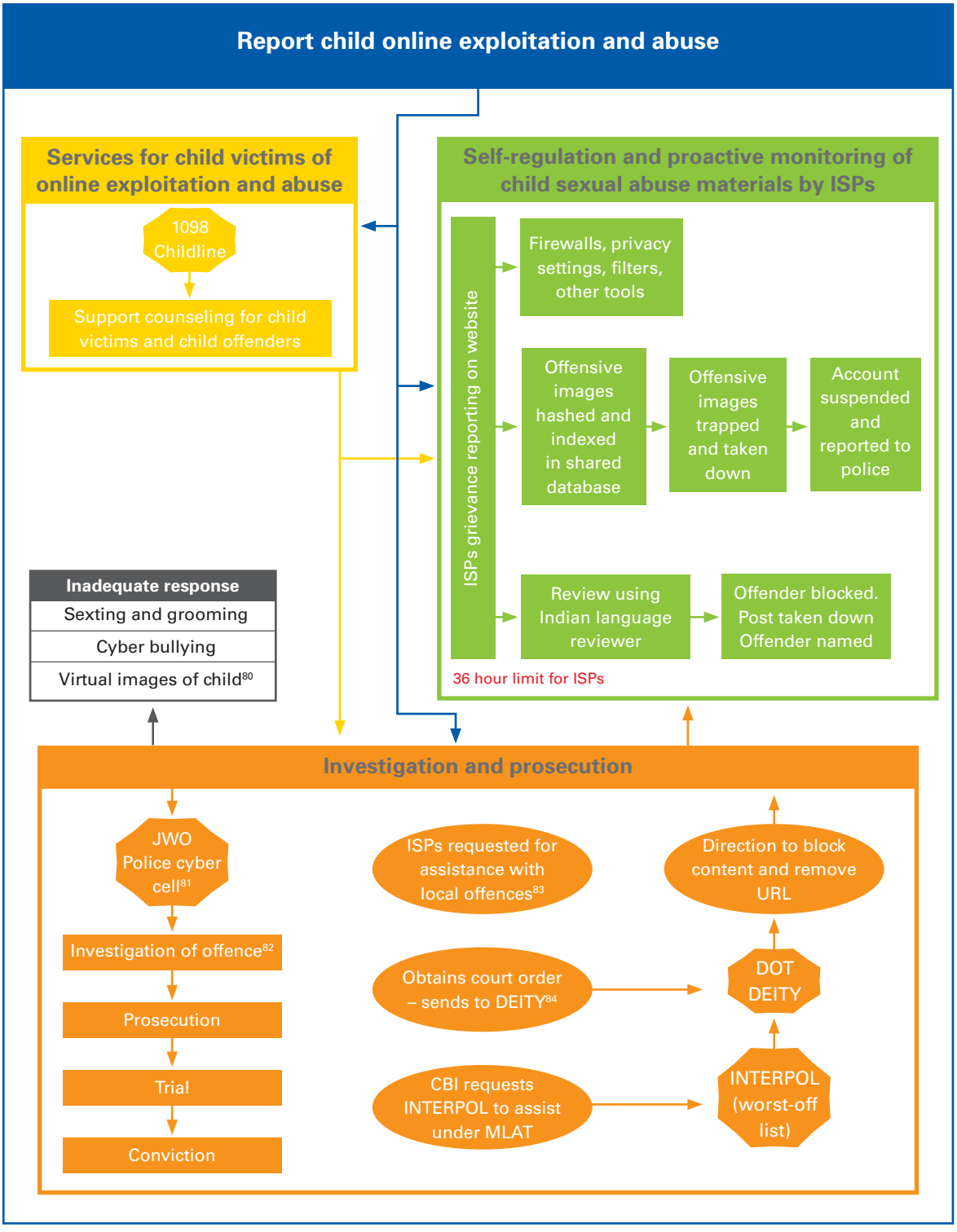
The invasion of privacy poses a serious ethical and moral challenge to the task of preempting and proactively addressing online offences

For the purpose of this assessment, three distinct areas of intervention were identified as follows:

1. monitoring, reporting and removing online child offensive material;
2. criminal investigation and prosecution of online sexual abuse and exploitation; and,
3. identification and service provision for child victims of online exploitation and abuse.

The combination of these three areas of intervention constitutes the emerging child online protection system in India; Figure 2 provides a map of the components and mechanisms to date under this system. Each section in this chapter provides a brief overview of the current systems and structures in place under each area as well as key challenges and areas for improvement.

Figure 2: Child online protection response system in India



[80] Grey areas in response. Such cases often not registered or investigated.

[81] Limited understanding of child online offences system wide.

[82] Inadequate forensic capacity to investigate online offences.

[83] Inadequate cooperation for international offences.

[84] No fixed time. Depends on urgency.

3.1 Monitoring, reporting and removing online child sexual abuse material

India presently lacks a mechanism for close monitoring, reporting and removal of online CSAM. As a result, data on the reporting and removal of CSAM also is not monitored or analysed and very few people would even know how to report CSAM as there is no guidance, protocol, hotline or coordinated response in place as yet. In order to guarantee prompt and effective removal of child offensive online material, strong collaboration between the ICT industry and law enforcement actors needs to be established.

To guarantee prompt and effective removal of child offensive online material, strong collaboration between the ICT industry and law enforcement actors needs to be established

Aarambh India, a Mumbai-based initiative supported by the NGO Prerana and ADM Capital Foundation, is collaborating with the United Kingdom-based Internet Watch Foundation (IWF)[85] to establish a national hotline for the reporting, removal and blocking of CSAM in India. The hotline is expected to be launched in the second half of 2016 via an anonymous reporting button on Aarambh's website (www.aarambhindia.org). IWF will screen reports and seek support from the ICT industry to remove the images and videos. Initiatives like this are critical at this point in time and long-term investment in a national sustainable India-based hotline, able to remove high volumes of CSAM, is needed.

In India, the National Technical Research Organization is responsible for critical infrastructure for internal and external security, with the Intelligence Bureau monitoring cases of terrorism and insurgency but not of child abuse. The National Central Bureau maintains a list of offending sites via INTERPOL India as well as the INTERPOL International Child Sexual Exploitation database. The Central Bureau of Investigation (CBI) cybersecurity cell monitors illegal content online but it does not monitor child sex abuse images.

The Indian Computer Emergency Response Team (CERT-In) is the national nodal agency responsible for issuing instructions to block websites.[86] It provides incident prevention and response services as well as security quality management services. While CERT-In responds to complaints, via a 24x7 operations centre that serves as a help desk for the police nationally, it does not monitor child online abuse material. CERT-In and the Centre for Development of Advanced Computing provide training on the procedures and methodology of collecting, analysing and presenting digital evidence for law enforcement agencies, forensic labs and the judiciary.

CSAM is reported to the police cybercrime cell which seeks clearance from the Department of Telecommunications and from the Department of Electronics and

[85] The Internet Watch Foundation (IWF) was established in 1996 by the Internet industry in the United Kingdom to provide a hotline to the public and IT professionals to report criminal online content in a secure and confidential way. In partnership with the online industry, law enforcement, government, and international partners, it works to minimize the availability of CSAM hosted anywhere in the world.

[86] CERT-In was set up under Section 70B of the Information Technology Act, 2000 to monitor Indian cyberspace and respond to cybersecurity incidents.

Information Technology (DEITY) to block the site containing the illegal content.[87] The time needed for this procedure varies depending on issues including: (a) the victim's willingness to report the crime; (b) the victim's awareness of where and how to report; (c) the understanding of the police regarding the nature of the offence; and (d) the policies of the websites hosting the offensive material. The illegal content is expected to be removed within 24–36 hours of reporting either by the victim him/herself or by any concerned person who may have come across such content. However, this timescale is hardly met as a court order is required to remove the content and the process to obtain the court order can take up to seven days. This procedure is only applicable to local sites and uniform resource locator (sRLs) or web addresses hosted in India. For sites hosted in other countries, CERT-In seeks linkages with counterpart bodies from other countries if a bilateral memorandum of understanding has been signed between the countries. A high level of international cooperation and assistance has to be established to effectively and promptly remove child sex abuse images.

CERT-In responds to complaints, via a 24x7 operations centre that serves as a help desk for the police nationally,but it does not monitor child online abuse material

It has been reported that India may approach INTERPOL to gain access to websites that engage in child pornography. This came after the Supreme Court expressed serious concerns over the issue. It also followed an unsuccessful attempt by the Indian Government in 2015 to ban 857 pornographic websites. DEITY established a Cyber Law and e-Security Group which includes representatives of the telecom department, CBI, the ISP association and officials from telecom operators such as Bharti Airtel, Vodafone and Telenor.[88] The CBI is expected to play a key role in the engagement with INTERPOL by

[87] The police are responsible for requesting a court order to block the illegal site and to write a letter to the designated Cyber Law Authority along with a copy of the court order. Then, with approval of the Director General of CERT-In and the Secretary of DEITY, removal of content and/or blocking of the URL is initiated. The service provider is requested to remove the URL.

[88] *The Times of India*, 'India to Turn Heat on child porn sites with Interpol aid', 16 March 2016. <http://timesofindia.indiatimes.com/india/India-to-turn-heat-on-child-porn-sites-with-Interpol-aid/articleshow/51419415.cms>

keeping tabs on websites that are engaged in child pornography. INTERPOL maintains a "worst of" list that has details on such websites and URLs that can be replicated and used by authorities in India. The INTERPOL list is updated frequently. Efforts will also be made to identify other international agencies that gather information on child pornography.[89] The ISPs have, however, advised that any request to block websites with child pornographic material must come through DEITY and not directly from the CBI.

The CBI is expected to play a key role in the engagement with INTERPOL by keeping tabs on websites that are engaged in child pornography

The Indian Cyber Crime Coordination Centre (I4C) was set-up to coordinate with multiple agencies and stakeholders to prevent and reduce vulnerability to cyberattacks and minimize damage and recovery time from such attacks when they occur. I4C has direct access to the Crime and Criminal Tracking Network and Systems and National Intelligence Grid, India's two largest databases for information related to national crime and criminals. There is a proposal for setting-up a separate unit within I4C to deal with online crimes against women and children. Tackling child sex abuse images and online abuse and exploitation will be the top priority for this additional unit, which will also monitor and block child sex abuse image sites.

The Indian Government's National Advisory on Preventing and Combating Cyber Crime against Children, 2012[90] has framed recommendations for action related to child online protection which, together with the recent announcements regarding the establishment of a National Cyber Crime Coordination Centre with a dedicated unit for cyber offences against women and children, are important indications of a growing understanding at the highest level of decision makers of the online threats to children and need for concerted efforts to address them. A coherent and coordinated response by all stakeholders will enable the building of a strong protective online environment for children.

Box 11: The darknet

The Darknet, or hidden web, is the space for most of the serious online offences against children. The Darknet, is recognized as the underworld or the "Wild West" of cyberspace and cannot be accessed using Google or other regular search engines. It requires special software products, such as TOR (The Onion Router). TOR provides a high level of anonymity on the Internet and renders a PC's net address untraceable. The data is encrypted in multiple layers, like an onion, and then sent across the Internet through multiple relays until it reaches its destination.

Social platforms, search engines and messaging platforms

Most social media platforms (e.g., one-to-one like WhatsApp or one-to-many like Facebook, Twitter, Instagram, Flickr, MySpace, etc.), search engines and ISPs have mechanisms for reporting abusive content and material. Offensive content is self-

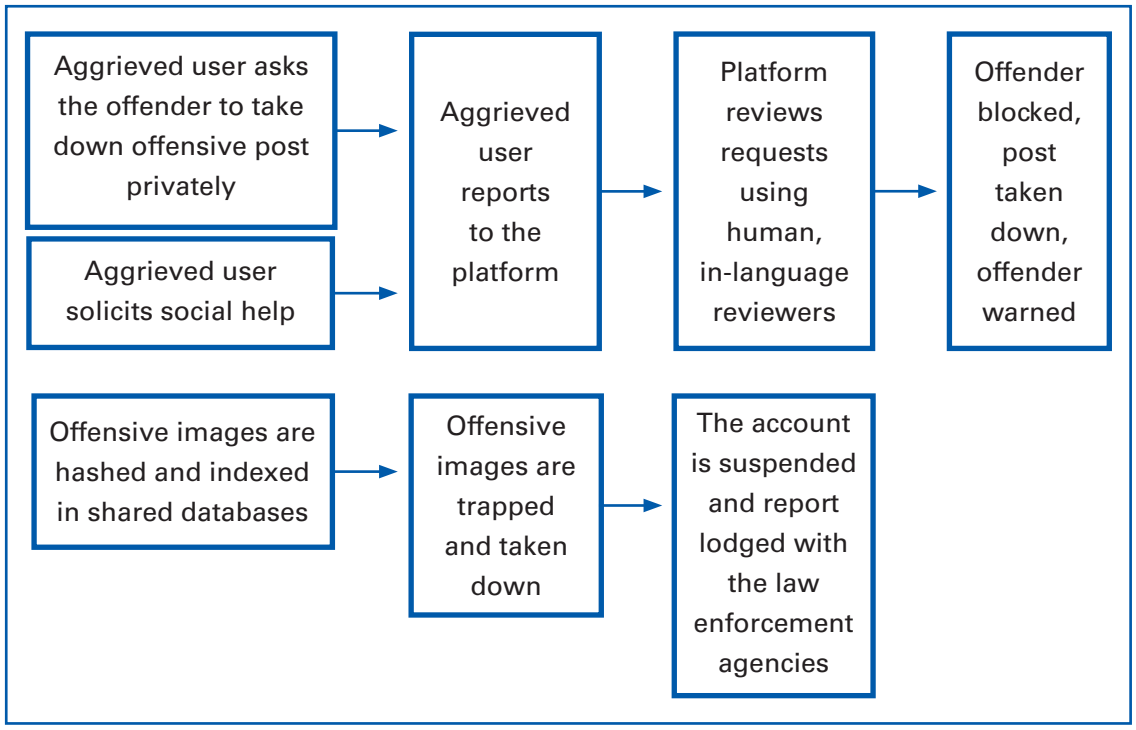
[89] Telephone discussion with Rakesh Maheshwari, Scientist G, Director DEITY, March 2016.

[90] See Annex 2: National Advisory on Preventing and Combating Cybercrime against Children.

regulated via filters, privacy settings and complaint mechanisms. For instance, Facebook, Twitter and Instagram have been investing in the safety of their platforms to ensure that they are not used for child sexual abuse and exploitation, and more generally for cybercrime or discrimination. Figure 3 offers a broad view of what a generic self-regulatory process used by a social media platform would look like.

Since 2011, social media platforms have been using Photo DNA technology developed by Microsoft to scan every uploaded photo to control the distribution of CSAM.[91] Child pornography images are deleted immediately and the account is blocked and examined by a team of experts. The images classified as illegal are added to a global photo DNA database. If there is reason to believe that a child is in immediate danger, the case is referred to a local law enforcement agency or reported to the National Center for Missing and Exploited Children (NCMEC) in the United States and the International Centre for Missing and Exploited Children elsewhere.

Figure 3: Generic self-regulatory processes of social media platforms



Some social platforms, like Facebook and Twitter, created reporting mechanisms to facilitate reporting, blocking of offensive content and warning of offenders. Facebook and Twitter now have safety information hubs for users to easily report abuse and access safety policies and guidance. Staff are trained to identify offensive content and appropriately refer it to a team of child safety experts. They also monitor the search engine for child exploitative terms and compile a list of the most common terminologies used to search for child abusive material.

[91] ECPAT International, Child Sexual Abuse Material. <www.ecpat.net/sites/default/files/SECO%20Manifestations_CSAM.pdhttp://www.ecpat.net/sites/default/files/SECO Manifestations_CSAM.pdf>

Search engines like Google and Bing also established mechanisms to block the search of illegal material on their engines. For example, the Google algorithm limits search results for suspected child sexual abuse queries, implements Microsoft's digital fingerprint technology to tag illegal images and detects film footage showing illegal activities. More specifically, the Google algorithm (which Google constantly updates) means that child sexual abuse queries do not yield results but lead to warning messages from Google that appear at the top of search results directing the individual to places where they can get help, such as charities.

Globally, Internet companies have been working with law enforcement for many years to stop illegal material being shared on the web. Generally, child sexual abuse images are removed and reported to the designated authorities. In order to coordinate these efforts, close collaborations have been built between Internet companies and NCMEC, the Child Exploitation and Online Protection Centre (CEOP) (United Kingdom), IWF, INTERPOL, the FBI and many local, federal and international law enforcement organizations and departments.

New challenges have now emerged with the rapid rise and adoption of over-the-top messaging platforms such as WhatsApp, Snapchat, WeChat and Viber. Such platforms have created a whole new ecosystem of use and potential abuse of children, given their person-to-person nature and removal of messages from servers once delivered. Mobile Internet access via pre-paid options, while convenient for consumers, create significant challenges for law enforcement as well as for service providers in tracking illegal behaviour and identifying offenders.

Over-the-top messaging platforms have created a whole new ecosystem of use and potential abuse of children, due to their person-to-person nature and removal of messages from servers once delivered

3.2 Criminal investigation and prosecution of online sexual abuse and exploitation

Cybercrime investigation is the domain of the police. However, few cases of cyber offences involving children either as victims or offenders are reported to the police, and even fewer reach the courts. Cyber offences against a child are reported at local police stations through police juvenile welfare officers or cybercrime cells of the law enforcement agency across the country. After registering a complaint with the local police station or cybercrime cell, any further redressal process for such cases is similar to that for other crime-related cases.

Inadequate knowledge of laws and limited enforcement capacities among law enforcement agencies

Limited awareness about the issues, discriminatory mindsets and inadequate familiarity with laws among front-line police officials undermines reporting and investigation of cases. The lack of understanding of the intricacies of cyber laws and laws aimed at protecting women and children is a reflection of inadequate training and deep-rooted societal prejudices. The front-line police official is not able to respond effectively when

the offence is reported, leading to the experience-based recommendation of cyber experts that senior officials should be contacted for dealing with the issue of jurisdiction and ensuring prompt action.[92] Front-line police officials also lack the basic knowledge of cyber forensics, resulting in poor preservation of evidence. The system of pre-service education and in-service training of law enforcement agencies has not been able to respond to the shortcomings in the legal framework, which require a nuanced understanding and application of various laws to address the ever-evolving and complex range of cyber offences.

Cybercrime cells and cyber forensic capacities

There are currently 23 police cybercrime cells in India.[93] Some states have one cyber cell while many larger states have more than one. These cyber cells are guided by the Code of Criminal Procedure for conventional crimes and a set of investigation manuals with procedures for search, seizure analysis and presentation of digital evidence in court. The standard operating procedures (SOPs) for cybercrime investigations and a Cybercrime Investigation Manual developed by the Data Security Council of India (DSCI) have been in use since 2011 and have harmonized the investigation processes. Cyber forensic laboratories are attached to some of the cyber cells for undertaking computer, network and mobile forensics and for training on cybercrime and cyber forensic evidence.

Cyber cells are guided by the Code of Criminal Procedure for conventional crimes and a set of investigation manuals with procedures for search, seizure analysis and presentation of digital evidence in court

Conviction rates for child online abuse are extremely low. One of the key reasons is the poor quality of evidence and the lack of police capacities to handle cyber evidence in

[92] Telephone conversation with Rakshit Tandon, India cybersecurity specialist, January 2016.

[93] Refer Annex 3: Cybercrime Investigation Cells in India

cases of child sexual abuse. For example, police have often not been trained to preserve e-mails as evidence in a case of child sexual abuse. They also often do not attach a 65B certificate due to which the evidence cannot be admitted in court. As a result, victims of online abuse are denied justice while perpetrators enjoy impunity.

Infrastructural and technological deficits do not allow forensic labs to deal with large volumes of evidence. There is a need to build the capacity of specialists for each branch of cyber forensics, and have notified labs as provisioned under the law. Usage of the Association of Chief Police Officers' Guidelines for Handling Digital Evidence has to be mainstreamed. Issues of cloud networks, self-destructive evidence and different data types and time zones pose a serious challenge, especially since cybercriminals are often technological masterminds who use different methodologies to eliminate all possible traces of their crime to evade detection. Policies on minimum qualifications and skills of cyber forensic experts are required together with extensive and higher levels of police training for handling cybercrime, especially on gathering and safeguarding the evidence. Recognizing private labs and partnerships with private forensic labs may help to clear long backlogs and strengthen cyber forensic agencies in the short term.[94]

Box 12: Safeguarding digital evidence

Digital evidence has its own set of challenges for law enforcement agencies, which lack proper guidelines on dealing with digital evidence and SOPs for child abuse cases. The following are broad principles that need to guide the handling of digital evidence.[95]

- Upon seizing digital evidence, actions taken should in no way alter the digital evidence. In cases where it is unavoidable, the actions should be satisfactorily accounted for.
- When it is necessary for a person to access original digital evidence, that person must be forensically and legally competent to do so.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review, if so ordered by the competent authority.
- An individual is responsible for all actions taken with respect to digital evidence while it is in his/her possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance to these principles.

[94] Sebastian Edassery, Director of Forensic Services, Deloitte Touche Tohmatsu India Private Limited. <www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html>

[95] Association of Chief Police Officers (ACPO), *Guidelines for Handling Digital Evidence*. <www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.> The National Institute of Standards and Technology of the United States Department of Commerce and the Scientific Working Group on Digital Evidence are other sources of best practices, technical notes and guidelines for forensic quality and consistency.

Industry associations such as the DSCI, established by NASSCOM, have helped to strengthen cyber forensic investigation and forensic capacities. In collaboration with DSCI, cyber forensic labs have been set up in Mumbai, Bangalore, Pune, Haryana, Chennai, Hyderabad and Kolkata to provide training on cybercrime investigation and awareness creation. Standardized manuals and cyber forensics tools have also been developed for the collection, analysis and presentation of digital evidence by law enforcement agencies. However, practitioners indicate that there are shortcomings in the system-wide availability and use of these tools in many states.

The Cybercrime Investigation Programme under the Police Modernization Scheme of the Ministry of Home Affairs is helping with the establishment of cybercrime police stations and cybercrime investigation and forensic training facilities in all states and union territories. The DSCI is also planning to assist with the establishment of two national centres of excellence in the area of investigation of cybercrimes and digital evidence.

The CBI Training Academy has set up a cyber forensics training lab to impart basic and advanced training in cyber forensics and investigations to police officers associated with the CBI. In addition, the Government has set up cyber forensic training and investigation labs in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu and Kashmir to train law enforcement officials and judiciary in these states. The cybercrime cells in Delhi, Mumbai and Chennai are said to be functioning well, while others struggle with inadequate capacities and facilities.

In-service police training

Reporting and registration of cybercrime is increasing but most police officials responsible for investigation of cases are either untrained or undertrained in cyber forensics. The National Police Academy conducts a few training courses on cybercrime

and forensics, but mainly for Indian Police Service (IPS) officers. State police training colleges train non-IPS officibut lack the requisite competencies for cyber forensics.

CERT-In and the Centre for Development of Advanced Computing provide basic and advanced training to law enforcement agencies, forensic labs and the judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

The CBI Training Academy in Ghaziabad has been conducting courses on cybercrime-related topics since 2006. It runs short courses on incident response, cybercrime investigation, computer forensics, mobile forensics, prosecution and vigilance for its own officers as well as the officers of state police and vigilance agencies between the levels of sub-inspector and deputy inspector general, but these are clearly inadequate to meet the requirement, given the large number of police officers to be trained. Various trainings on child exploitation and online protection for CBI officers as well as state police officers are also conducted at regular intervals at the CBI Academy, Ghaziabad, in collaboration with UNICEF, CEOP, the Governments of the United Kingdom and France and various Indian NGOs and consultants. In addition, in 2010 the Ministry of Information Technology set up a Cyber and Hi-Tech Crime Investigation and Training Centre at the CBI Academy to address the need for computer and mobile forensics services for all Indian law enforcement agencies, including capacity-building in areas such as proactive monitoring of offenders sharing CSAM within the local jurisdiction, i.e., India/states/various cities.[96]

The National Law School of India University (NLSIU) in Bangalore recently started an advanced certificate course on 'Cybercrimes, cyber law and cyber forensics', including a module on collecting digital evidence in social media. The course is currently being attended by 104 CBI officers.

The Ministry of Home Affairs proposes to train approximately 100,000 law enforcement functionaries to address cybercrime in 2016-2017

While cybercrime investigations pose a challenge for the older generation of policemen and policewomen who are less proficient with ICT and the Internet, new police recruits are more adept and many of them even have relevant academic qualifications.[97] The cyber forensic investigation talent pool is expected to improve with an ambitious capacity development initiative of the Ministry of Home Affairs, which proposes to train approximately 100,000 law enforcement functionaries to address cybercrime in 2016-2017.[98]

Pre-service legal education

Cyber law has not as yet been integrated sufficiently in the curriculum of any of the 100 law colleges in India. As a result, lawyers are not adequately equipped to handle cyber offences. The Indian Law Institute and private universities like Amity offer some courses on cyber law to students with a specific interest in the subject. There are, therefore, only a few lawyers with specialization in laws dealing with children as well as cyber laws.

[96] <www.cbiacademy.gov.in/chcit.phphttp://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html>

[97] Interview with Mohd. Taj Hassan, Special Commissioner for Crime, Delhi Police, 18 January 2016.

[98] Interview with Kumar Alok, Joint Secretary, Ministry of Home Affairs, 12 October 2015.

Judicial processes

There are no special or fast-track courts for cyber offences and the justice system is already overloaded with the backlog of cases. The Protection of Children from Sexual Offences Act covers some aspects of cyber offences against children and 605 special courts have been set up under the Act across the country;[99] however, there is inadequate confidence in the capacity of these courts to handle sexual assault/child sexual abuse cases. According to the feedback reported from several states and a recent study of the special fast-track courts for sexual assault and child sexual abuse cases in Karnataka, there is a critical need for training on dealing with sexual assault cases for prosecutors, judges and other participants in the criminal justice system, with specialized and ongoing training on violence against women as a minimum provided to judicial officers, prosecutors, lawyers and registrars.[100] In this scenario, the potential contribution of these courts to handle child online abuse cases cannot be relied upon.

The National Judicial Academy, Bhopal, and 21 state judicial academies conduct occasional orientations on cyber laws for the judiciary. The NLSIU in Bangalore and the NALSAR University of Law in Hyderabad also conduct awareness and training programmes on cyber laws and cybercrimes for judicial officers. Not only are these trainings inadequate to meet the existing and growing requirements, the training of prosecutors is an exceptionally weak link in the justice system. They are currently not included in police training or judicial trainings. They need to be trained and updated on cybercrime, especially cyber offences against children, in a systematic manner.

[99] Press Information Bureau, Government of India, Ministry of Women and Child Development, 3 March 2016. This information was given by the Minister for Women and Child Development, Mrs Maneka Sanjay Gandhi, in reply to a question in the Rajya Sabha.

[100] Kothari, Jayna and Aparna Ravi, *The Myth of Speedy and Substantive Justice: A Study of the Special Fast Track Courts for Sexual Assault and Child Sexual Abuse in Karnataka*, Centre for Law and Policy Research, Bangalore, 9 June 2015.

The Cyber Appellate Tribunal, earlier known as Cyber Regulations Appellate Tribunal, was established in October 2006 in accordance with provisions under Section 48 (1) of the Information Technology Act, 2000. As per the Information Technology Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an adjudicating officer under the Act can prefer an appeal before the Cyber Appellate Tribunal. There is a Cyber Appellate Tribunal constituted under the Information Technology Act situated at New Delhi, but a judge to preside and decide on the cases has not been appointed since 2011.

International cooperation

The challenges of jurisdiction in the online environment make it necessary to create formal mechanisms, agreements and memorandums of understanding for international cooperation. While the Indian authorities are able to elicit support from Indian ISPs, they challenge the claim of social media platforms, search engines and ISPs that operate as per global protocols and United States laws (where most of these servers are located), as well as in accordance with local laws. The Indian authorities cite difficulties in getting international ISPs to cooperate with investigations in accordance with Indian laws, especially offences that are transnational in nature or involve actors in other countries.

The transnational nature of cybercrime calls for international cooperation. The United States has often failed to share or facilitate information vital to dealing with cybercrime. It denies access to information held by companies that are based in the United States such as Google, Microsoft, Facebook, etc. on the grounds that it would be in contravention of its laws.[101] Indian laws like the Information Technology Act do not apply to United States firms. INTERPOL steps in at the request of CBI to facilitate investigations in support of prosecuting cases under mutual legal assistance treaties (MLATs), but before their assistance is sought, the initial investigation should be thorough and involve preservation and security of evidence. This remains a lacuna in India.

With growing advances in technology, it is difficult to attribute the origin of attacks and to ascertain the identity of the perpetrators of cyber offences. Moreover, the anonymity offered by ICT and the Internet allows perpetrators to impersonate and cover their tracks. This emboldens more users to experiment with ICT abuse for criminal activities, which blunts the deterrent effect created by legal frameworks such as the Information Technology Act, 2000 and other well-intended actions for enhancing cybersecurity in India. In view of the legal jurisdictions of different countries and entities, the investigation and resolution of cybercrimes are often delayed due to shortfalls in international cooperation. DEITY enters into international cybersecurity cooperation arrangements with organizations engaged in similar activities, in the form of memorandums of understanding. Where no such agreement exists, the provisions of a MLAT are used to elicit support for cybercrime cases.

Anonymity offered by ICT and the Internet allows perpetrators to impersonate and cover their tracks, emboldening more users to experiment with ICT abuse for criminal activities. This blunts the deterrent effect created by legal frameworks

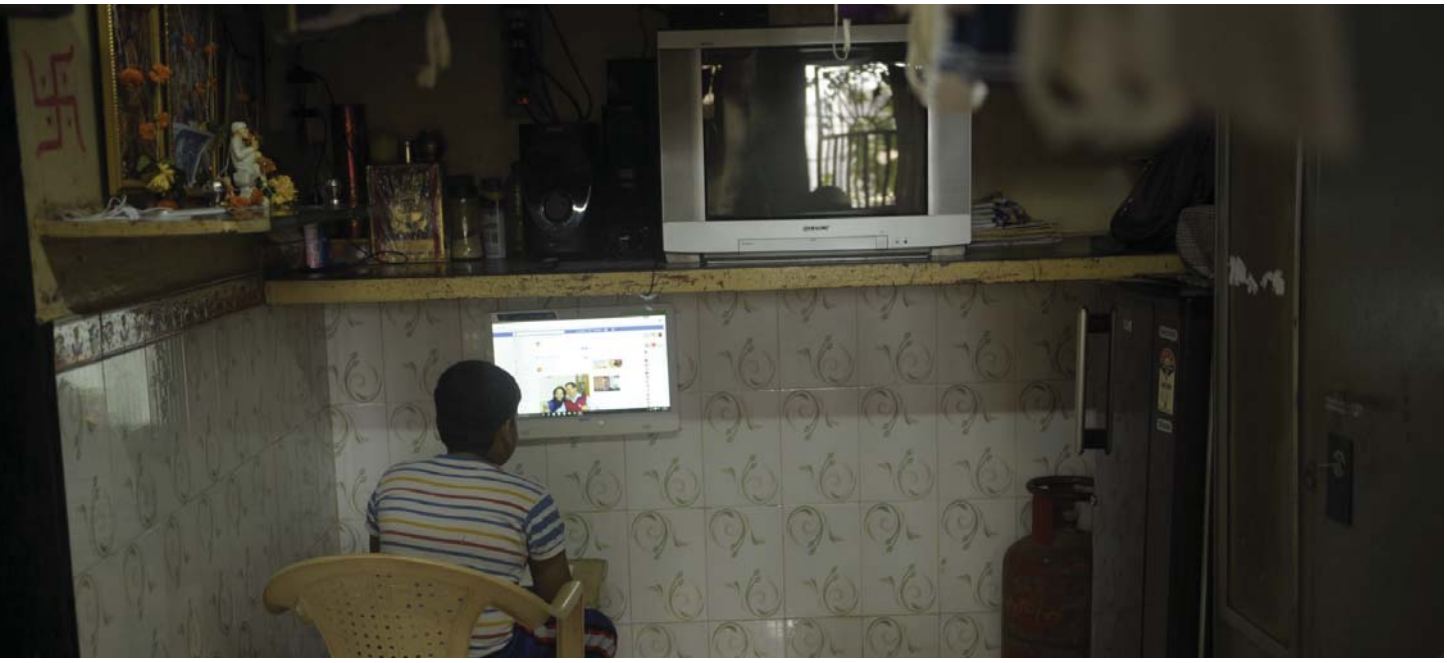
[101] Interview with Kumar Alok, Joint Secretary, Ministry of Home Affair, Government of India, 12 October 2015.

Child pornography and child trafficking syndicates involving commission of crime in more than one jurisdiction warrant close cooperation from international and domestic law enforcement bodies. In several instances, the victims, children and women, have approached international hosting websites directly, stating that their pictures or videos have been posted online without their consent and in violation of intellectual property rights, and the hosting websites have taken down the illicit content within 24–36 hours. However, investigative logs were provided only after police requests were sent through official channels.

The MLAT which India has signed with various countries is not effective for cybercrime investigation and prosecuting cases that require international cooperation. The timelines for response are not quick enough to seize, preserve and produce the electronic evidence, which is fragile and easy to tamper with. Due to resulting delays, evidence is either not collected in time or extradition is not possible. Indian policies and legislations on cyber-crime need to be aligned with relevant international agreements and conventions, especially the ones targeting children, like the WePROTECT Global Alliance.[102]

3.3 Identification, reporting and services for child victims of online exploitation and abuse

In principle, children and adults can report an online offence against a child either directly to the police or via Childline India by dialing 1098. In practice, according to various accounts, lack of sufficient understanding of cyber offences among front-line police



[102] Recommendation from the Child Online Protection Workshop with the Private Sector, New Delhi, 8 February 2016, and the Expert Consultation on Child Online Safety in India, New Delhi, April 2016 hosted by UNICEF India. The 70 countries involved in the WePROTECT Global Alliance have committed to work together to end child sexual exploitation online. Specifically, they are working towards a common set of aims which are to: (a) identify victims, and ensure they receive necessary support; (b) investigate cases of exploitation and prosecute offenders; (c) increase public awareness of the risks posed by children's activities online; and (d) reduce the availability of child sexual abuse material online. WePROTECT Global Alliance, Our Strategy to End the Sexual Exploitation of Children Online, 2016.

officials deters complainants, while inadequate capacities and competencies among inspectors and sub-inspectors hinder investigations. Childline India, the 24-hour helpline for child victims of violence, abuse and exploitation, is another forum for reporting a cyber offence against a child in a confidential manner.[103] Childline India reports cyber safety complaints to the police cybercrime cell for further investigation and appropriate response.

In the past year, Childline India noted a significant increase in the reporting of child online abuse cases and it is currently facing challenges in providing an adequate response. This is mainly due to the lack of knowledge, skills and competences of key professionals to respond to cases of child online abuse. In principle, the National Commission for the Protection of Child Rights (NCPCR) or the state commissions may also be approached for redress as they have a special role in monitoring the implementation of the Protection of Children from Sexual Offences Act. However, knowledge and capacity deficits limit their ability to respond to technology-based child rights violations. A special orientation package could be developed for supporting their appropriate response in the area of online safety and violations of children's rights.

Providing an adequate response to the increased reporting of child online abuse cases via Childline India has proved challenging

Once the case is reported, establishing jurisdiction and securing evidence for investigation and prosecution are major challenges at the level of police stations. Approaching the cybercrime cell by engaging directly with senior officials seems to be the preferred route for cyber experts who are called upon for help by desperate victims and their families. Legal experts and law enforcement agencies highlight the practical difficulties in dealing with electronic evidence in cases that do get reported. Following the Supreme Court's landmark judgement in the PV Anvar vs PK Basheer case in September 2014, any electronic evidence or computer to be presented in court under Section 65B of the Evidence Act requires certification by a person holding a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.

Pavan Duggal, a cyber-law expert and advocate, avers that the introduction of the high burden of proof in the law has a detrimental impact on provision of electronic evidence in child online abuse cases. A person in a case of child pornography or abuse cannot be expected to provide certification that may be self-incriminating and in violation of Article 20 of the Constitution, which states that no person can be forced to give any evidence that is self-incriminating. He also notes that the process involved in taking a First Information Report (FIR) from the stage of prosecution to conviction poses another challenge to the effective enforcement of existing laws. He states that the majority of people who approach him for legal advice do not wish to lodge a legal complaint of online abuse of children as they fear social stigma and insensitivity from law enforcement agencies and reporting mechanisms.

[103] Childline India currently serves 350 districts and towns and plans to expand to 600 districts by 2019.

Underreporting of child online abuse

The National Crime Records Bureau (NCRB) and other monitoring mechanisms do not reflect the actual incidence of cyber offences against children in India but only those that are reported. Therefore, this information is significant only for tracking and inferring the performance of the law enforcement system. Online threats and offences against children are generally underreported for a variety of reasons. The current redressal system that relies on reporting of online offences against children and the lack of public awareness about what constitutes online violence and how to complain or seek assistance, combined with a lack of awareness of rights, poses barriers to reporting. This is not only limited to children and online crimes but it is also present in other spheres of life in India. For instance, the United Nations Broadband Commission for Digital Development, in its report on 'Combating Online Violence against Women and Girls', stated that 35 per cent of women in India reported their victimization while nearly 18 per cent were not even aware that they had been victimized.

The current redressal system combined with lack of public awareness about what constitutes online violence, how to complain or seek assistance and lack of awareness of rights, poses barriers to reporting

Given the context in which children are often unaware that an offence has occurred for which they can seek justice, the identification and reporting of online offences by children or adults is rather limited. Some of the underlying causes of non-reporting of online offences in India are as follows:

- Online offences are viewed as minor and not harmful to the child (e.g., emotional violence and not very severe physical harm). Adults tend to downplay their gravity by also factoring the investment of time and resources required in seeking specialized assistance or engaging with law enforcement agencies with no guarantee of an adequate outcome.
- For cases that are considered to be serious (e.g., generally offences that are sexual in nature), reporting may be considered a non-option due to fear of stigmatization of the victim. For instance, when reporting abuse, girls risk being blamed for their real or perceived role in the occurrence of the offence.
- Children fear that reporting may unleash bans and controls which further constrain the spaces available to them, especially girls. Sporadic but frequent reports of community groups restricting the mobility and means of communication for girls are indicative of this challenge.
- Guilt or fear may prevent children from reporting, especially when they are aware of having breached the rules or trust of adults. In such cases, children may prefer to seek help from their peers instead of approaching adult family members, school teachers or authorities.
- Very often, children do not know whom to approach if they decide to seek help. Most of the adults in their immediate surroundings are unlikely to comprehend the nature and magnitude of the problem and law enforcement agencies often do not foster confidence, especially among children and young people.

- Formal platforms, processes and procedures for identifying and responding to online abuse cases in schools are lacking.

The Parliamentary Committee on Information Technology in its report in 2014 identified the need for DEITY to expedite follow-up with the Ministry of Home Affairs to increase awareness among people regarding the mechanism of reporting cybercrime cases with the cybercrime cells of law enforcement agencies. The Committee also advised the Government to take up projects and schemes to raise children's awareness of cybersecurity on a continuous basis. It requested DEITY to take necessary action in coordination with the concerned authorities to make cybersecurity a mandatory part of the school syllabus. The Committee also recommended that DEITY set up a national helpline to guide the general public about dealing with cybercrimes and accessing redressal mechanisms.[104]

Data collection and analysis

Law and order being a state domain, all actions related to crime, including cybercrime, are dealt with by respective states/union territories and relevant data are maintained by the NCRB. The main function of NCRB is to collect, compile and disseminate information on crime, criminal tracking and missing persons in respect of various offences on the basis of monthly returns from state/union territory police authorities. A weak recording system is, therefore, a challenge for analysis and action-oriented discussions. Annual NCRB reports on crimes against children do not collate information on cybercrime or ICT-related offences against children under the Information Technology Act, 2000 and the IPC. While they provide data on cybercrime and IT-related offences, lack of disaggregation does not allow the estimation of children involved. The provisions of the POCSO Act can be applied in cases of online sexual abuse and exploitation but disaggregated information about cases registered under this Act are not available with NCPCR, which has the mandate for monitoring implementation of the law. The NCRB does, however, inform that 67 cases were booked under the Information Technology Act and 74 under the Indian Penal Code (IPC) against children for IT-related offences, and three arrests were made on charges of child pornography in 2014. While these figures may provide an insight on the enforcement of the law, they do not reflect the actual incidence of online abuse and exploitation.

The Parliamentary Committee on Information Technology identified the need to increase awareness among people regarding the mechanism of reporting cybercrime cases and taking-up of projects and schemes to raise children's awareness of cybersecurity

Although cybercrime cells are expected to monitor cybercrimes, the collated data and analysis are not available. The data made available annually by the NCRB are essentially a compilation with considerable scope for improvement in quality. Inadequate police response to cases of offline and online offences against children, due to lack of sensitization, orientation and relevant skills for investigation and prosecution, undermine the quality and utility of the data generated by the states and collated at the national level.

[104] *The Times of India*, T'ribal teen stripped in Birbhum, molested by hundreds', Kolkata, 9 August 2010. <http://epaper.timesofindia.com/Repository/getFiles.asp?Style=OliveXLib:LowLevelEntityToPrint_TOI&Type=text/html&Locale=english-skin-custom&Path=TOIKM/2010/08/09&ID=Ar00101>

Improvement in data gathering, collation and analysis is expected with the establishment of the Crime and Criminal Tracking and Network System. This nationwide system, using state-of-the-art technology to support investigation of crime and detection of criminals, is expected to enable the recording of all cases registered at police stations in all the states, including cyber offences. Their consolidation and generation of reports will also facilitate searches in response to specific queries. It is expected to be fully functional in 2016.

Services for child victims of online exploitation and abuse.

India has only a few facilities for children involved in cyber offences and these tend to have limited outreach and uneven quality of service. Existing facilities and specialized capacities for counselling and rehabilitation are concentrated in urban areas only, leaving vast parts of the country unserved. Even where specialized mental health experts are available for individual counselling, in large cities such as Delhi, Mumbai, Bangalore and Chennai, they have the capacity to reach only a small fraction of urban children in need of support, who can afford commercial counselling services.

The juvenile justice administration lacks counselling services for underage online offenders and there is no standard response protocol for cases of online abuse and exploitation within the education system. Capacity development initiatives for functionaries of the Integrated Child Protection Scheme do not as yet include the management of online abuse and exploitation cases. However, training modules are due to be revised in 2016 and it is expected that content on cyber safety will be included as part of the revision process.

A few initiatives of civil society organizations also respond to the needs of child victims of online exploitation and abuse. NGOs like Tulir (Chennai) and the Aarambh India Initiative (Mumbai) work for prevention of child sexual abuse by highlighting the issue as well as offering a range of support services to those involved. They have been at the forefront of the discourse on child online protection in India, and direct delivery of services complements their advocacy for policy response, resources and coordinated action. Another NGO, the Centre for Cyber Victim Counselling (CCVC) based in Tirunelveli, Tamil Nadu, works for cyber victims, helping them to understand the nature of the crime and providing legal and police assistance and counselling support.[105]

Some Internet "de-addiction" centres have been set up in India. The National Institute of Mental Health and Neuro Sciences set up a "Services for Healthy Use of Technology Clinic" to offer counselling support to help addicted persons to replace excessive technology usage with healthy usage. An Internet de-addiction centre was also set-up by the Delhi-based Uday Foundation two years previously to counsel children and parents and to wean them away from excessive use of the Internet by engaging them in social welfare activities. This free service has handled approximately 100 cases of Internet addiction in the last two years, with a significant population of younger children seeking assistance.

[105] Dr. Debarati Halder, CCVC Director, raises awareness regarding various types of cyber victimization and ways to cope with the situation through two blogs <http://debaraticyberspace.blogspot.com> and <http://cybervictims.blogspot.com/>.

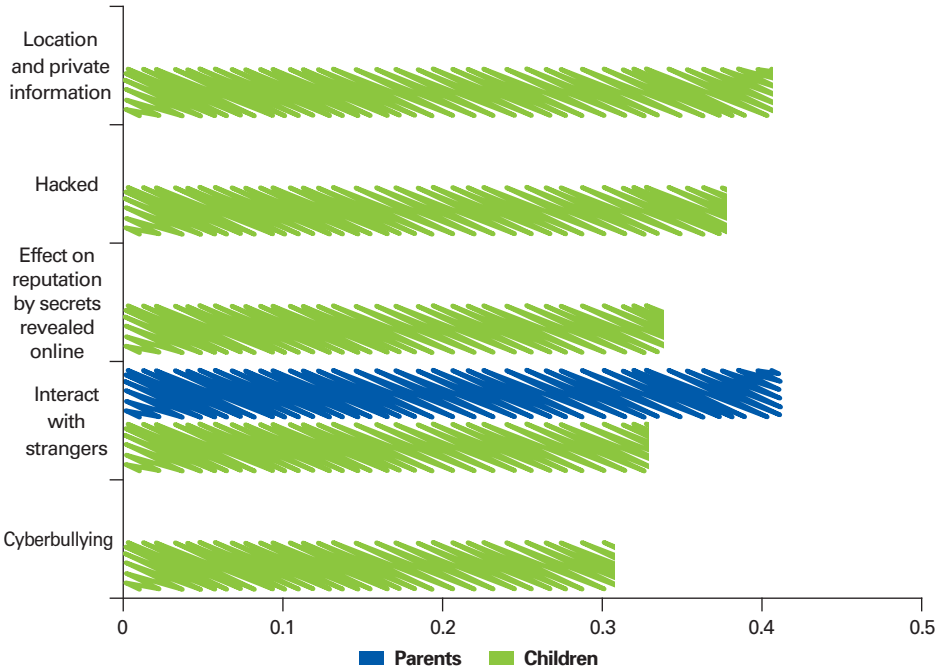
4. Prevention through education for digital literacy and safety

As discussed in the previous chapters, a unique set of issues is emerging as a result of the expansion of ICT and use of the Internet. Dynamic technology and the irrelevance of national boundaries to the transfer of information in cyberspace make it nearly impossible to control access. The affordability and accessibility of mobile phones further provides a level playing field to "haves", "have nots" and "have lots," giving them greater agency than ever before. As a result, it is imperative to inform children and parents about potential threats and safeguards to influence their use of digital devices and technology. A protective family environment also demands an open dialogue, negotiation and coordination based on a shared understanding of the risks of online social networking, protective capacity of communities and families and their own life skills, knowledge and participation.

One of the key gaps identified as part of this assessment is the lack of understanding of the risks and threats posed to children by ICT and social media among professionals, policymakers and society as a whole. Children often indulge in a wide array of risky behaviours online that remain undetected by the parents, as early exposure to ICT and social media has made them more adept than their parents at using technology in their daily lives.

Research among urban Indians reveals that children and parents are equally concerned about online risks. Sharing of personal information and its ramifications was predominant, followed closely by contact with strangers online. While parents and children are universally aware of the prevalence of online risks, children demonstrate a wider spectrum of awareness of those risks. This awareness gradient is perhaps explained by digitally native children habitually seeking information online as well as in conversation with their peers, both offline and online.

Graph 8: Perception of the worst things that can happen online



About 60 per cent of parents across eight metro areas shared that their children had consulted them about things that bothered them online. Despite claims of asking parents about online risks, almost two thirds of children keep some aspects of their online behaviour a secret from their parents. When asked, most children say they do not want their parents to know what they do with their friends. Clearing browsing history, deleting messages, using privacy settings, using mobiles instead of desktops or laptops and minimizing the browser in the presence of an adult are among the many stratagems used to safeguard their privacy.[106]

Most children and parents do not understand the full extent of the risks. In the United States, for example, parents largely seem to be content using offline means and discipline to protect their children online, eschewing available online tools and apps. Indian parents, with relatively lower levels of sophistication, show similar behaviours. Norton Security, a firm dealing with online security and protection, found that awareness of risks among adult Indians was significantly lower than global levels of concern based on the "it won't happen to me" syndrome. The same misplaced confidence probably extends to the risks faced by children online.

Children appear to share their concerns with parents primarily when encountering cyberbullying, either as a witness or victim. Parental engagement in informing and

[106] Intel Security, *Teens, Tweens and Technology Study*, Delhi, 2015.

educating them about online protection is limited. Very few claim to report, fewer still challenge the bullies and a substantial proportion do nothing.

Children and young people have a large role to play in safeguarding themselves and their peers from child online abuse

Experiences from other countries show that children and young people have a large role to play in safeguarding themselves and their peers from child online abuse. Examples of a few promising practices include the constitution of peer groups in schools called cyber congress, scouts or cyber security ambassadors. However, such practices have not been properly documented in India and there is little understanding of how digital literacy and safety programmes can be implemented effectively.

It is commonly argued that technological innovations would provide the best response given the technological nature of the challenges. The ICT sector has a key role to play in the prevention of, and response to, child online abuse and exploitation. However, it is clear that no single sector or agency can ensure the safety of children from online or ICT-mediated violence. Relevant government institutions, the private sector, international organizations, academia and civil society need to work together to build structures, mechanisms and capacities to prevent and respond to child online abuse, violence and exploitation in India. A safe online ecosystem for children requires a high degree of preparedness, collaboration and coordination among the stakeholders as well as adequate technological solutions.

The role of the Government

DEITY, part of the Ministry of Communications and Information Technology, has launched a five-year project on information security education and awareness. One of the activities under this programme is to widely promote information security awareness among

children, home users and non-IT professionals. C-DAC Hyderabad, which has been assigned the responsibility of executing this project, is expected to prepare information security awareness material and coordinate with participating institutes to organize various events. Useful information for children, students and parents is made available through messages, periodic competitions on safety issues and a website (www.infosecawareness.in). CERT-In also disseminates information and creates awareness on security issues through its website (http://www.cert-in.org.in) while police cybercrime cells undertake outreach activities in schools to raise awareness about the safe use of the Internet.

The role of the ICT sector

Many ICT companies and service providers conduct periodic surveys with the objective of improving and expanding the quality and reach of their services. The understanding of emerging trends in the behavioural and usage patterns of the users enables ICT companies to take strategic decisions about their products and to provide a better and safer experience to existing and potential consumers. It is worth noting that while available surveys provide interesting insights, they have tended to be confined to relatively high-end, urban ICT and Internet users. There are few enquiries covering different sociocultural and economic groups and these are usually limited to certain geographical areas. However, ICT companies and service providers can play an important and critical role in preventing and responding to child online abuse and exploitation. Some companies in India have already started to play a key role in addressing the issue.

ICT companies and service providers can play an important and critical role in preventing and responding to child online abuse and exploitation

The DSCI, a body set up by NASSCOM, has been conducting social awareness campaigns to inform and educate individuals and end users, including children, in Tier II and Tier III cities[107] about cybersecurity and cybercrimes through week-long social awareness campaigns. These campaigns use open group discussions, quizzes and conferences to target students, home users and working professionals. Cyber labs under DSCI also conduct some outreach programmes in schools. A school outreach programme was conducted for students and parents in collaboration with Telenor.

IAMAI has organized outreach programmes on safe web surfing and digital wellness through a consultant reaching approximately 100,000 students in schools and colleges over the last five years. Individual schools have cyber safety champions advising children on online safety and netiquette.[108]

Intel Security's Cybermum is a digital evangelist who champions the cause of online safety for children through an active blog on Wordpress, the Intel Security portal, Twitter and Facebook. With about 600 Facebook friends and over 13,400 followers on Twitter,

[107] Tier II cities have a population of 1 million and Tier III cities have a population of less than 1 million.

[108] Rakshit Tandon has reached 1.5 million students through a safe surfing programme since 2008, and currently supports Cyber Congress in about 100 schools. He has been supported by IAMAI, Facebook, Intel and Telenor in this effort. His Facebook page on safe surfing provides a platform for responding to queries.

Cybermum has a follower base comprising parents, academicians, parent bloggers and other parent influencers. She analyses popular studies and their relevance for children and has blogged about issues such as cyberbullying. Since September 2014, Intel Education's Digital Wellness Curriculum has been providing digital education among schools in India in an effort to ensure grassroots education on cyber safety and digital wellness. In 2014 alone, the programme reached over 108,000 students in India.

Telenor's Webwise initiative seeks to introduce first-time users and young children to the potential of the Internet for information and learning but also informs them of the online risks and threats of bullying, abuse and malware. A Telenor report highlighted that Indian children face the worst risks due to a combination of high rate of access to mobile phones and low resilience due to a lack of formal or informal counsel to create awareness of or control over their Internet activity. In response, Telenor started a school outreach programme aimed at creating awareness of Internet safety among children and helping parents to monitor and educate their children about Internet safety. The programme, named WebWise, was started in February 2014 with Telenor volunteers reaching out to schools and parents to run Internet safety workshops for children. The first phase of the programme reached 15,000 children and the initiative continued into 2015.

As part of the India Digital Literacy and Internet Safety Campaign, Google's Web Rangers programme empowers teens to promote safe use of the Internet among their peers. Web Rangers are students who have been equipped to serve as ambassadors for safe and responsible use of the web in their schools. They are trained to create cyber safety campaigns among their peers to encourage thinking about online behaviour and how to keep each other safe online. The initiative enrolled young people aged 14–17 years, representing 50 schools in Hyderabad, Bangalore and New Delhi.

Microsoft's Stand Up To Online Bullying quiz and Digital Citizenship in Action toolkit, in conjunction with the results of the 2012 Global Youth Online Behaviour Survey, provide adults with tools and resources to help start the conversation with children about how to stay safer online. The quiz is designed to walk adults through a series of scenarios in which, upon answering, they receive immediate guidance on how to talk about, identify and respond to the range of online behaviours from meanness to bullying and beyond. The toolkit is an interactive educational guide which teaches users about responsible use of technology.[109] Microsoft also partners with organizations like iKeepSafe, iLookBothWays and the Anti-Defamation League to provide professional development to teachers and school staff with courses on online bullying, public awareness campaigns and cyber safety education.

The role of civil society

Few civil society organizations have chosen to address child online protection issues, which can be attributed to a deficit of technological know-how required to meet the complex and ever-evolving nature of cyber offences against children. Agencies that have engaged with child online protection issues have either been working against child sexual abuse and exploitation, for meaningful education, or seek to highlight critical emerging social issues.

Few civil society organizations have chosen to address child online protection issues, which can be attributed to a deficit of technological know-how required to meet the complex and ever-evolving nature of cyber offences against children

Chennai-based Tulir-Centre for the Prevention and Healing of Child Sexual Abuse has extended its offline work for public awareness on child sexual abuse, prevention and support services for child victims and policy advocacy related to the online space. It provides guidance and support to child victims of online exploitation and abuse, whether the cases are registered with the police or not. In addition, Tulir lobbies for the integration of cyber safety in the school curriculum in Tamil Nadu and advocates against online abuse and exploitation of children at the national and international levels.

New Delhi-based Breakthrough has used the digital space for its media campaigns and dialogue with young audiences against gender-based violence and discrimination. The group has also taken up issues of online harassment and violence against women and girls and methods for addressing them. Breakthrough has used the online space to create a dialogue with young boys and girls to examine their own beliefs and social norms related to gender relations and violence against women and girls.

The Cyber Peace Foundation incorporated child online protection in its programs via two initiatives: the 'E-Raksha Seminars' in schools to raise awareness of children of the risks and threats when using internet and social media; and, the 'I-Safe Project' specifically targeting youth to sensitize them on cyber-abuse, cyber-harassment and cyber-extremism implemented in collaboration with the Policy Perspective Foundation

[109] The interactive online quiz and the toolkit can be downloaded as a teaching tool by organizations and schools.

Bachpan Bachao Andolan ran an online campaign on child sexual abuse called Full Stop in 2015. This included aspects of online abuse and exploitation of children including cyberbullying, cyberstalking and sexting. The information addressed children, care providers and survivors of sexual abuse online and offline through a school outreach programme. The group's specific focus is on online child sexual abuse, trafficking, child pornography and extortion through engagement with key stakeholders on the international dimensions of child trafficking.

Freedom from Abuse of Children from Technology (FACT), the brainchild of the Asian School of Cyber Laws, provides information for parents and children on some of the threats that exist online and safe behaviours to mitigate them.

Although civil society organizations are doing a commendable job of creating public awareness about digital safety and building resilience among children to deal with potential harm online, the narrow focus or limited reach of their initiatives does not adequately address the growing need for informed and responsible use of technologies. Taking these interventions to scale remains a major challenge. A coordinated response – including common content focus, sharing of lessons and the evolving concerns of children through a common platform, coordination of action and resources, institutionalization through inclusion in the school curriculum, and peer education – could guide the way forward.

Partnerships between the ICT industry and civil society

A number of initiatives for digital safety, digital wellness, netiquette education and awareness programmes have been initiated by ICT companies and service providers in collaboration with civil society organizations. For instance, Facebook has been working with NGOs on programmes and guides for adolescents and parents on how to stay safe online and offline. Moreover, the Safety Centre on the Facebook site seeks to help people learn about how to stay safe while using the platform.

Both Google and Facebook have supported the Learning Links Foundation (LLF), which works actively with education stakeholders, leaders and policymakers to improve education systems, enhance curricula, reform assessments and leverage technology solutions to enhance teaching and learning processes. LLF has been able to reach 300,000 students over 11 years of age with cyber safety and wellness awareness in 19 states of India. The partnership with Facebook has resulted in Internet safety campaigns reaching 52,000 students in 10 states. The much older partnership with Google has led to the cybersecurity Web Rangers programme in 15 states. In November 2015, the Family Online Safety Institute recognized LLF for its outstanding work on online safety.

Twitter is developing the "Twitter for Good" initiative with five vertical areas dealing with freedom of expression, women in technology, emergency crisis response, improving access and inclusion, and digital citizenship focusing on privacy, safety and prevention of

child sexual exploitation. Its outreach programme for women in technology seeks strong collaboration with organizations working for women's empowerment and rights to deal with issues of harassment and vitriolic abuse.

The Mumbai-based initiative, Aarambh India, works on the issue of child sexual abuse. Its website is the first national resource portal on online child sexual abuse and exploitation, which it seeks to locate within the broader framework of child protection in India and elsewhere. It also has a separate section on online safety for children with videos and other resources. Aarambh provides support services for child victims of online abuse and exploitation. Recognizing the threat posed by websites that carry CSAM, it is collaborating with the United Kingdom-based IWF. A reporting button on its website links to the IWF hotline for reporting CSAM. IWF assesses material and, if illegal, takes steps to remove it.

Box 13: Digital citizenship: Preparing children for a digital world

There is an urgent need to address and mitigate the risks associated with widespread use of ICT (i.e., online threats, abuse and misuse of information, and physical and mental health hazards) while simultaneously taking advantage of the opportunities afforded by these technologies. Children and young people in a digital world need to be equipped with appropriate knowledge, skills and attitude to leverage and enjoy the potential benefits of ICT while being resilient to the risks.

The concept of digital citizenship helps teachers, technology leaders and parents to understand what children, students and users of technology should know to use technology appropriately and responsibly. More than a teaching tool, it is a way of preparing them for current challenges. The proactive approach of digital citizenship education could foster a favourable environment to encourage responsible and safe use of ICT among children and youth with support from schools, teachers, parents/guardians, policymakers, industry leaders and other key stakeholders.[110] The following are some of the critical components of digital citizenship education:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying and digital drama
- Digital footprint and reputation
- Self-image and identity
- Information literacy
- Creative credit and copyright

[110] <www.unescobkk.org/education/ict/resources/publications/elibrary-themes/teaching-and-learning/fostering-digital-citizenship-through-safe-and-responsible-use-of-ict>

5. Legislation and policies to protect children online

5.1 Existing policies and laws

The policy and legal framework for cybersecurity in India is evolving and, notwithstanding several shortcomings, is fairly enabling. It can be used effectively even with its limitations to build a comprehensive strategy and action plan for addressing the issue of child online protection in the country through concerted and coordinated efforts by various stakeholders.

The Information Technology Act, 2000 addresses several aspects related to cyberspace in a relatively comprehensive manner with provisions for compliance and deterrence. The provisions of the National Cyber Security Policy,2013 enable the development of a dynamic legal framework. The periodic review of the implementation of the policy, the Information Technology Act, 2000 and other related legislation may help in addressing the cyber security challenges arising from technological developments in cyberspace.

To begin with, the Constitution of India provides for special legislation, policies and interventions for children. The provision of protecting children from abuse can be interpreted to include online abuse, which allows for the establishment of appropriate

legal protection and systems. Based on these commitments, children are to be given opportunities to develop in a healthy manner with freedom and dignity. This allows for access to opportunities through ICT for learning and development, while being protected from possible harm. The State is responsible for ensuring that children are protected from exploitation. This is an enabling provision for building systemic measures to protect children from possible exploitation through ICT.

Although online risks due to ICT represent an emerging challenge for the protection of children in India, the National Policy for Children (NPC), 2013 does not refer to them directly. The broad parameters of the policy implicitly allow for measures to ensure equal access to opportunities for all children through ICT with appropriate safeguards. It affirms the Government's commitment to the rights-based approach in addressing the continuing and emerging challenges in the situation of children (Section 1.5). It also articulates the "State's commitment to take affirmative measures – legislative, policy or otherwise – to promote and safeguard the right of all children to live and grow with equity, dignity, security and freedom, especially those marginalized or disadvantaged; to ensure that all children have equal opportunities; and that no custom, tradition, cultural or religious practice is allowed to violate or restrict or prevent children from enjoying their rights" (Section 2.2).

The broad parameters of the National Policy for Children implicitly allow for measures to ensure equal access to opportunities for all children through ICT with appropriate safeguards. However, the policy does not directly refer to the challenge posed by online risks to children

All policies, whether related to education, ICT or cybersecurity, are expected to incorporate the principles and measures laid down by the NPC to provide children with equal opportunities for learning and empowerment, while building safeguards for their protection from possible harm. The provisions in the education section of the NPC emphasize safety and a safe learning environment, and the use of ICT and equal access to ICT by all children. These are enabling provisions for a balanced approach to providing appropriate opportunities for accessing information, participation and building safeguards for protecting children from potential risks and harm from the online environment.

Protection from online abuse can be interpreted through the provisions requiring protection of children from all forms of violence, abuse and exploitation. The provisions do refer to protection from pornography. Section 4.12 highlights a preventive and responsive child protection system and preventive measures and punitive action against any form of exploitation and abuse. Section 4.13 focuses on access to redress mechanisms. In all, the protection provisions provide for a comprehensive and systemic approach to address the issue of child online protection.

The NPC also articulates children's participation in issues affecting them based on their evolving capacities. Section 4.14 emphasizes that "The State has the primary responsibility to ensure that children are made aware of their rights, and provided with an enabling environment, opportunities and support to develop skills, to form aspirations and express their views in accordance with their age, level of maturity and evolving capacities, so as to enable them to be actively involved in their own development and in

all matters concerning and affecting them". The emphasis on appropriate opportunities to enable children to be actively involved in their own development also implies equitable opportunities through ICT for learning and empowerment and fully equipping children with the knowledge to protect themselves from potential harm.

The National Policy of ICT in Schools,2012 is more explicit about regulating ICT to protect children from potential risks. It recognizes that "access to the Internet enhances the risk of inappropriate content reaching children and compromising privacy and identity of individuals" and provides for evolving appropriate advisories for regulating access, monitoring Internet activity and education. This includes privacy and security of students and teachers, training of the heads of schools and teachers in appropriate security and regulatory measures, and monitoring of children's access to ICT.

Promotion of ICT systems in school and adult education is a thematic area in the section on school education in the new National Education Policy being developed by the Ministry of Human Resource Development through broad-based consultations. The draft policy reportedly emphasizes the potential of ICT to improve the quality of education and build the capacities of teachers to develop appropriate educational content, but does not address the ways and means of reducing the potential risks and harm to children from ICT, including informed and safe user behaviour. This is clearly an area for advocacy with the Government during the ongoing process of policy development and finalization.

Advocacy is needed to ensure that the new National Education Policy being drafted by the Government directly addresses the ways and means of reducing potential risks and harm to children from ICT

The mission, objectives and provisions of the National Cyber Security Policy, 2013 address dimensions of prevention, investigation and prosecution of cybercrime,

including cybercrimes against children. It emphasizes the strengthening of capacities and capabilities of law enforcement agencies for investigation of cybercrimes and collection of critical data to enable prosecution. The importance of responsible user behaviour underscored by the policy, implying their knowledge of online risks and exercise of appropriate precautions, is particularly critical for children using ICT and the State (Government) is obligated to create this awareness and knowledge. The provision for audit of security measures is important for assessing the effectiveness of measures taken by various service providers to safeguard children's use of ICT. Section 11 focuses on enabling effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention. Section 12 emphasizes the creation of a culture of cybersecurity and privacy enabling responsible user behaviour and actions through an effective communication and promotion strategy. In addition, Section D, on strengthening the regulatory framework, mandates periodic audits and evaluation of the adequacy and effectiveness of the security of information infrastructure. Under the provisions for human resource development, Section 1 seeks to foster education and training programmes both in formal and informal sectors to support the nation's cybersecurity needs and build capacity and Section 2 stresses the establishment of institutional mechanisms for capacity-building for law enforcement agencies.

The National Cyber Security Policy (2013) addresses dimensions of prevention, investigation and prosecution of cybercrime, including cybercrimes against children

The Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008 are the main pieces of legislation concerned with online activities. Inclusion of the term "communication device" covers any communication device used to transmit any text, video, audio or image, i.e., mobile phones, computers, iPads/tablets, gaming consoles or similar devices. The amendment in 2008 broadened the scope of the original law and clarified the scope of some provisions.

The law identifies the following as online offences against children:

- Transmission and publication of obscene material, i.e., child pornographic material or otherwise adult content in electronic form;
- Transmission or publication of sexually explicit acts in electronic form (including any adult content video, MMS, short clip or image including 'self-clicked images');
- Transmission or publication of material depicting children in sexually explicit acts in electronic form or creating images, text, collecting, seeking, downloading, advertising, promoting or distributing content that depicts children in an obscene or sexually explicit manner;
- Enticing a child or children into an online relationship for sexually explicit acts or in a manner that can offend a reasonable adult, or facilitate abuse of children or recording in electronic form own abuse or that of others relating to a sexually explicit act with children. The provisions cover child pornography, grooming, sexual predation, sex webcam recording and live webcam streaming of sexual conduct;

- Intentionally or knowingly capturing or publishing or transmitting images of a private area of any person with or without his or her consent as it violates the privacy of the person (includes clicking a picture of oneself or a person with consent and posting it on any communication device in nude or semi-nude form);
- Securing access to a computer without authority, downloading or copying data (data theft), introducing a virus or causing damage to a database or programme, disrupting access, tampering with a computer in any way, charging services to another person, destroying evidence or similar activities with the aim of causing damage;
- Dishonestly receiving any computer resource or communication device, identity theft, i.e., making use of someone's password or electronic signature, cheating by personation (through blogs, fake profiles, false e-mail addresses and fake images) and breach of confidentiality and privacy by sharing or making private information public.

The Indecent Representation of Women (Prohibition) Act, 1986 also prohibits indecent representations of women in various forms and criminalizes the performance of obscene acts and songs with imprisonment of up to three months but does not punish the audience or those who make the person perform such acts.

The provisions of the Information Technology Act have been fortified by the Protection of Children from Sexual Offences Act, 2012 which deals with several online offences against children, including child pornography and grooming

The provisions of the Information Technology Act have been fortified by the Protection of Children from Sexual Offences Act, 2012 which deals with several online offences against children, including child pornography and grooming. Media, hotels, photographic studios, clubs, hospitals, etc. are legally bound to report any child pornographic material. The following are offences under the law:

- Sexual harassment of a child by showing any object in electronic form for pornographic purposes, or repeatedly making contact with a child digitally or threatening the child to use any form of media (Section 11 (ii), (iii) and (iv));

- Using real or simulated images of a child for pornographic purposes or enticing of children for sexual gratification or pornography (Section 13(a), (b) and (c));
- Using or engaging a child in any medium like print, electronic, computer or any other technology for preparing, producing, offering, transmitting, publishing, facilitating and distributing pornographic materials (Section 13(a), (b) and (c));
- Storing any pornographic material in any form involving a child for commercial purposes (Section 15);
- Abetment to commit any of the above offences (Section 16).

As the Information Technology Act does not have specific provisions for offences such as criminal intimidation, hate speech and defamatory content, the provisions of the IPC are applied in cases of online offences. These include: Section 153A (hate speech or sedition); Section 419 (cheating by impersonation); Section 420 (cheating); Section 500 (defamatory content); Section 506 (criminal intimidation); Section 507 (criminal intimidation by anonymous communication); and Section 292 (prohibition on possession of obscene material). The application of IPC in conjunction with the Information Technology Act, however, can contribute to problems of interpretation and challenges the capacities of law enforcement officials and the judiciary.

The Information Technology Act also provides guidelines for cybercafes by insisting on the proof of identity; an adult accompanying a child; and the use of commercially available safety or filtering software to avoid, to the extent possible, any access to websites relating to pornography, including child pornography or obscene information. In addition, cybercafes are mandated to maintain identity proof of users, user logs and necessary documents and data for a period of one year. Cybercafes are also mandated to display a board, clearly visible to users, disallowing them from viewing pornographic sites, as well as copying or downloading information that is prohibited under the law according to the IT (Guidelines for Cyber Café) Rules, 2011. Cybercafes are expected to immediately report to the concerned police if they have reasonable doubts or suspicions regarding any user.

These provisions do not have the desired effect in the absence of active supervision, monitoring and registration of cafés. In the absence of effective monitoring of these facilities and revoking of licenses in case of default, there is no information regarding the effective application of these guidelines, the nature of breaches in procedures and resulting issues impacting child online protection in these public facilities.

The Information Technology Act and Information Technology (Intermediaries Guidelines) Rules address intermediaries' liabilities for making available third-party content. The Information Technology Act generally protects intermediaries from being liable for transmitting or hosting third-party information, data or communication links made available by them (Section 79 (1)) if they exercise due diligence (Section 79 (2)) and

observe the Information Technology (Intermediaries Guidelines) Rules. However, an intermediary is liable for the acts performed by the third party if: (a) the intermediary has conspired or abetted or aided or induced the commission of the unlawful act provided under the Information Technology Act; or (b) the intermediary receives actual knowledge or is 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 unlawful acts, but fails to immediately remove or disable access to the materials in any manner (Section 79(3)).

The Information Technology (Intermediaries Guidelines) Rules detail the duties of intermediaries with due diligence mentioned in Section 79 (2) of the Information Technology Act. Intermediaries, upon finding out that information which is obscene, pornographic, harmful for minors or illegal is located on their computer systems, are required to disable such information within 36 hours; and preserve such information and associated records for at least 90 days for investigation purposes (Section 3 (4)).

Although the Information Technology Act has provisions for establishing data retention and preservation requirements for intermediaries, the legal system only provides specific rules on data retention related to the identification of users of public computers in cybercafes and their history of website access. Intermediaries are required to preserve and retain such information as may be specified for such duration and in such manner and format as the central Government may prescribe (Section 67C) but these rules have not yet been promulgated by the Government.[111]

Box 14: Benchmarking Indian laws for child online protection

In its 2016 Global Review of Legislation on Child Pornography, the International Centre for Missing and Exploited Children presented six criteria to assess the adequacy of national laws for protecting children: (a) Does national legislation exist with special regard to child pornography? (b) Is child pornography defined? (c) Are computer-facilitated offences criminalized? (d) Is simple possession of child pornography criminalized? (e) Are ISPs mandated to report suspected child pornography? (f) Are there data retention provisions that require ISPs to retain digital user-data for purposes of prosecuting online criminal activity?

Indian laws appear adequate when tested against these parameters, but for many Indian legal experts and law enforcement agents the challenge is application of the law to prosecute offenders. The available legal provisions do not provide adequate protection to children due to differences in terminology and definition, lack of standard operating procedures and guidelines, and inadequate capacities of law enforcement agencies.[112]

[111] World Bank, *Protecting Children from Cybercrime. Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying.* A joint report of the World Bank and ICMEC, 2015.

[112] Pavan Duggal and Karnika Seth at the Expert Consultation on Child Online Safety in India organized by UNICEF in New Delhi, 8–9 April 2016. Also <www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html>

5.2 Limitations of policies and laws

A range of provisions in the law address child online protection but their effectiveness is undermined by the lack of clear definitions; grey areas emanating from cultural perceptions of what is right and wrong, acceptable and unacceptable or obscenity and decency; and the reality of inequitable gender relations.

5.2.1 Lack of a uniform terminology

Universal terminology on online abuse and exploitation of children is considered imperative for clear and effective communication and public discourse on the issue as well as in the interpretation and application of law and the framing of comprehensive protection through policy and law. The absence of a common terminology to define conduct that is absolutely unacceptable compounds the inherent complexities of child sexual abuse and exploitation and hinders efforts to protect children. Disagreements regarding the actual meaning of terms have created confusion and challenges for policy, legislation, interventions and public advocacy.

Disagreements regarding the actual meaning of terms have created confusion and challenges for policy, legislation, interventions and public advocacy

Furthermore, legal instruments defining and criminalizing sexual exploitation of children through ICT have not kept pace with new modalities of sexual exploitation of children through ICT. Key legal instruments in some instances predate important technological advances. For example, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the leading international instrument prohibiting sexual exploitation of children, does not criminalize live-streaming of child sexual abuse or online sexual grooming.

The new global terminology guidelines ("Luxembourg Guidelines"), which are now available to all major child protection agencies and organizations around the world, as well as lawmakers and the media, have introduced standard interpretations of terminology. Through practical guidance on navigating the complex lexicon of commonly used terms relating to the sexual abuse and exploitation of children, including their online dimensions, they seek to inform the discourse and collaboration on a common framework for child protection.

5.2.2 Lacunae in the law

Certain shortcomings in Indian laws need to be recognized and addressed notwithstanding the fact that the legal framework is by and large fairly enabling and can be invoked to address several cyber offences against children. Advocate Karnika Seth avers that the extant Indian laws are not sufficient to effectively prevent and combat the various cyber threats of cyberbullying, cyberstalking and sexual abuse involving grooming, sexting and child pornography that children are exposed to in a digital world. Many acts such as sexting and cyberbullying that have been criminalized in other countries are not as yet considered to be offences under Indian law.[113]

[113] Karnika Seth, Expert Consultation on Child Online Safety in India, hosted by UNICEF, New Delhi, 8-9 April 2016.

Indeed, establishing certain forms of cyber harassment as legal offences poses a challenge due to the lack of legal provisions for addressing cyberbullying. While laws criminalize child trafficking with the intent of sexual exploitation, they do not specifically address and criminalize child trafficking with the intent of producing pornography and advertising child sex tourism online. Judicious application of legal provisions, e.g., the provisions for intimidation and harassment for cyberbullying and sexual exploitation for pornography, may provide the way out. But the law does not recognize extraterritorial jurisdiction over child pornography offences when the victim is an Indian and is silent on the criminal liability of children involved in pornography. It also does not establish the confiscation of proceeds derived from child pornography offences.

Indian law possibly criminalizes possession of child pornography without the intent to distribute although the law uses the term "storage" and "collect" rather than "possession" of child pornography. Section 15 of the Protection of Children from Sexual Offences Act criminalizes storage of any pornographic material in any form involving a child for commercial purposes.[114] Section 67 B (b) of the Information Technology Act makes creation of text or digital images, collection, seeking, browsing, downloading, advertising, promotion, exchanging or distribution of material in any electronic form depicting children in obscene or indecent or sexually explicit manner punishable offences.

The Information Technology Act may also not have explicit provisions that require ISPs to report child pornography on their networks[115] but Section 19 (1) of the Protection of Children from Sexual Offences Act requires any person (including a child) who has apprehension that an offence under this Act is likely to be committed or has knowledge that such an offence has already been committed, to provide such information to the Special Juvenile Police Unit or the local police. As stated above, Section 13 of the same Act explicitly prescribes that activities using children for pornographic purposes shall be an offence. Moreover, Section 14 (1) of this Act punishes any person who contravenes Section 13 of the same Act.

[114] World Bank, *Protecting Children from Cybercrime. Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying*. A joint report of the World Bank and ICMEC, 2015.

[115] Mathew, Lina Acca, *Online Child Safety from Sexual Abuse in India*, J. OF INFO. L. & TECH. at 12. <www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/mathew/mathew.pdf>

Establishing the criminality of grooming and sexting is difficult and probably not desirable in view of the potential for misuse of the law. Distinguishing grooming from conversations that result from increasingly intimate relationships or genuine enquiries and exchange of information and views based on shared interests is difficult and for this reason it cannot be termed outright "mal-intentioned" or "illegal". Forging friendships and courtship rituals do incorporate an element of grooming but the risk element is quite strong.

The stages of grooming are important from the perspective of child protection as it can lead to undesirable and/or illegal actions, but Indian laws do not use the term "grooming" explicitly. They do however have provisions for dealing with enticement of children. The Protection of Children from Sexual Offences Act on sexual harassment implies grooming through Section 11(vi), which deems the action illegal when someone "entices" a child for pornographic purposes or gives gratification thereof. Section 67B (c) of the Information Technology Act also makes it illegal for anyone to "cultivate, entice, and induce 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.

Children and adults need to be educated about exercising caution as grooming can be the path to potential harm, and sexting and self-exposure can enhance their vulnerability manifold. While the law addresses obscene language or text, sexting and self-exposure remain grey areas.

A contentious issue is the matter of a child's consent. The law has specified that in matters of sexual abuse, issues of consent of children under 18 years do not arise.[116] Keeping in mind the trends among adolescents of sexting, sharing of selfies and willful exposure, which may be a willing action from both sides, what will happen in the event of exploitation arising from these acts? Will both children be criminalized or treated as victims requiring counselling and guidance on avoidance of risky online behaviours? Advocate Karnika Seth underscores the need to amend Indian laws to combat child trafficking through the Internet because the extant laws, such as the Immoral Traffic Prevention Act, 1956, the Information Technology Act, 2000 or Protection of Children from Sexual Offences Act, 2012, do not address this problem.[117]

A contentious issue is the matter of a child's consent. The law has specified that in matters of sexual abuse, issues of consent of children under 18 years do not arise

Registrars of domain names are not obliged to check the identity and particulars of the registrant under any extant legislation in India. As a result, registrants often submit fictitious names and addresses to register misleading and deceptive websites that target children and lure them into pornography and other obscene content online. Registrants are under an obligation not to use websites for illegal purposes but there is no way to catch the offenders as information submitted by a registrant is mostly incorrect or false.[118]

[116] Government of India, Protection of Children from Sexual Offences Act, Delhi, 2012.

[117] Karnika Seth at the Expert Consultation on Child Online Safety in India, organized by UNICEF India, Delhi,April 8–9, 2016. <www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html>

[118] Ibid.

Pavan Duggal, a cyber-law expert and advocate, notes that although the Information Technology Act, being a special law, has an overriding effect and prevails in the event of any inconsistency of its provisions with the provisions of the IPC or the Protection of Children from Sexual Offences Act, it does not have sufficient teeth to provide children with comprehensive protection. He believes that considerable effort is needed to review the Information Technology Act to address the problems being faced in the detection, investigation and prosecution of cases involving child online abuse.

5.2.3 Subjective interpretation of legal provisions

There is considerable scope for subjectivity in interpretation of legal provisions pertaining to online safety of children, particularly in the absence of SOPs/guidelines for Indian law enforcement agencies, including police and cyber forensic labs, to handle digital evidence related to illicit images/videos of sexually exploited children. Furthermore, when the victims are not available, proving the age of the child who is close to maturity is also very difficult based only on images and videos.

when the victims are not available, proving the age of the child who is close to maturity is also very difficult based only on images and videos

The striking down of Section 66A of the Information Technology Act, 2000 by the Supreme Court of India as unconstitutional is a classic case of the perils of subjectivity and threats to basic human rights articulated in the Fundamental Rights of the Indian Constitution. The Supreme Court held that Section 66A introduced by the 2008 Amendment to the Information Technology Act curtailed a citizen's constitutional right to freedom of speech and expression and gave police sweeping powers to arrest anyone for posting "annoying" or "offensive" comments online.

This case highlighted the potential of ICT to strengthen freedom of expression, the role of media in highlighting the breach of this fundamental right and the judiciary's role

in rendering unconstitutional any legal measures that undermine fundamental rights. But it also underscored the challenge of enacting legal provisions that can be applied objectively and balancing freedom of expression with protection of children and women in particular. Posting defamatory and inflammatory content online is still punishable under the IPC. The Court said that procedural safeguards in the criminal procedure code already exist to ensure they are not misused.

Box 15: Section 66A of the Information Technology Act

In March 2015, the Supreme Court of India struck down Section 66A introduced by the 2008 Amendment to the Information Technology Act on the grounds that it curtailed a citizen's constitutional right to freedom of speech and expression. The Amendment was aimed at preventing the misuse of information technology, particularly through social media, and Section 66A provided for up to three years of imprisonment and a fine for persons convicted for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet.

However, extremely wide parameters allowed subjective interpretations by law enforcement agencies. Most of the terms used in Section 66A were not specifically defined under the Act. The term "offensive" has a very wide connotation and could be subjected to varied interpretations. Something innocuous for one person could be offensive for another to merit a complaint and if the police prima facie accepted the latter view, an arrest could be made under Section 66A.

Application of Section 66A in several cases, especially in 2012 and 2013, resulted in outrage and protests. These included the arrests of: two girls in Maharashtra by Thane Police in November 2012 over their Facebook comment regarding the shutdown of Mumbai for the funeral of Shiv Sena chief; a Jadavpur University professor for forwarding caricatures on a Trinamool Congress chief on Facebook; an activist for drawing cartoons lampooning Parliament and the Constitution to depict their ineffectiveness; two Air India employees from Mumbai for allegedly posting offensive comments against politicians on their Facebook group; and a businessman by Puducherry police for an allegedly offensive tweet against the son of a former finance minister.[119]

A batch of legal petitions alleged that Section 66A trampled upon the fundamental right to freedom of speech and expression and asked that it be declared unconstitutional. The main argument was that it was a potential tool to gag legitimate free speech online. It curtailed the right to freedom of speech and expression guaranteed by the Constitution and exceeded the ambit of "reasonable restrictions" on that freedom.

[119] <http://indianexpress.com/article/india/india-others/sec-66a-21-individuals-who-changed-the-system>

The role of intermediaries and points of Internet access (e.g., hotels, malls and cafes) in protecting children online is another area that requires attention and clarification.

Karnika Seth proposes that India should consider incorporating a mandatory obligation on intermediaries (and also credit card companies) to report online child sex abuse incidents. In addition, the due diligence guidelines for intermediaries under Section 79 of the Information Technology Act, 2000 should provide effective parameters for blocking and pre-filtering CSAM; the adequacy of the data retention period by websites/ISPs (time period) should be reviewed; and rules under Section 67C of the Act should specify a log-retention period.

Pavan Duggal concurs that the Government needs to issue specific guidelines on Section 79 of the Information Technology Act to direct intermediaries on the specific steps they need to take to protect children from potential online abuse/threats. In addition to this aspect, detailed attention and clearly defined guidelines are also required for Section 13 of the Protection of Children from Sexual Offences Act, which considers "using real or simulated images of the child for pornographic purposes or enticing of children for sexual gratification or pornography" to be an offence but does not clarify if cartoons, sketches, drawings, virtually created images and animation are included.

5.2.4 Balancing protection and privacy

Children's right to privacy is commonly pitted against their right to protection. There has always been a strong narrative in India that questions the imperative of privacy in the Indian social milieu and considers it to be a luxury in congested and limited spaces, which is now being complemented by the emerging narrative on public security.

Box 16: Banning pornographic websites: How effective can they be?

There was outrage on social media as well as in mainstream media when the Government banned 857 websites in August 2015, following the Supreme Court's observation that "appropriate steps" were needed against pornographic sites, especially those featuring child pornography. DEITY asked the Department of Telecommunications (DoT) to notify ISPs under the Information Technology Act to disable the sites. DoT relied on Section 79(3)(b) of the Information Technology Act to order the blocking of these sites. Section 79 lays down conditions under which ISPs or intermediaries are exempt from culpability for offensive content uploaded by a third party. It obligates the intermediaries to exercise "due diligence" and to act on the orders of the court or the Government and its agencies to qualify for immunity. The DoT order stated that the content hosted on porn sites related to morality and decency and therefore was subject to "reasonable restrictions" on the fundamental Right to Freedom of Speech and Expression.[120]

[120] By order no. 813-7/25/2011-DS (Vol.-V), DEITY asked DOT to notify ISPs to block access to 857 URLs, under the provision of Section 79(3)(b) of the Information Technology Act, 2000 as the content hosted on these websites relates to morality, decency as given in Article 19(2) of the Indian Constitution.

Protection often requires proactive measures, including surveillance, which tends to intrude upon the right to privacy. A common narrative on where the boundaries should be drawn based on a public debate is not likely to emerge any time soon.

5.2.5 Children accused of cyber offences

How persons below the age of 18 years accused of cyber offences are to be treated by law in view of the proliferation of laws dealing with related issues needs to be subjected to a thorough enquiry. Developing approaches that do not criminalize children and adolescents for harmful online behaviours is essential.

Such cases have not as yet appeared in the public domain but are entirely plausible as the Information Technology Act, 2000 is silent about the definition of a child except when the child is a victim of sexual exploitation. The recently amended Juvenile Justice (Care and Protection) Act, 2016 states that if a child below 18 years of age but above 16 years of age commits heinous crimes, he or she may be tried as an adult upon the recommendation of the Juvenile Justice Board.[121] However, it is silent about cyber offences committed by children.

Developing approaches that do not criminalize children and adolescents for harmful online behaviours is essential

Many children open accounts with social networking sites even if they are not entitled to do so, with or without the consent of their parents. Social networking sites such as Facebook prescribe 13 years as the minimum age to register as a user and it is a standard form of contract. However, only someone who has completed the age of 18 years can enter a contract under the Indian Contract Act. Falsifying age for the purpose of entering into a contract amounts to misrepresentation under Section 18 of the Indian Contract Act and misrepresentation of one's own identity is an offence under the Indian Penal Code. These legal provisions are applicable to the virtual world as well. The implications for children of misrepresentation of identity and parents of abetment need to be considered, especially if Juvenile Justice Boards are required to review such cases.[122]

[121] Section 15 of the Juvenile Justice (Care and Protection) Act, Delhi, 2016.

[122] Kesavamoorthy, R., 'Legal Study on the Protection of Children in Social Network: Special Reference to Indian Law', *OSR Journal Of Humanities And Social Science* (IOSR-JHSS) Volume 15, Issue 1, Sep. - Oct. 2013. <www.Iosrjournals.Orghttp://www.iosrjournals.org>

6. Conclusion

The proliferation of ICT and the expansion of the "Internet of Things" are becoming indispensable for social and economic interactions for the majority of the world's population. The rapid adoption of ICT witnessed in India, together with the Government's plans for Digital India, call for urgent adoption of a strategic approach. Such an approach has to be enabling, proactive and build capacities for taking advantage of the immense opportunities afforded by these technologies for children and their development and participation. At the same time, approaches have to minimize and mitigate the risks associated with ICT use for children's safety, protection of privacy, potential exploitation and their physical and mental well-being.

Although not much is known about the actual prevalence of cyberbullying, online sexual abuse and exploitation, cyber extremism, cyber addiction and other risks and threats for children, it is evident that Indian children are being affected in many ways

The protection of children from violence, abuse and exploitation is a major concern in India, but there is an inadequate knowledge base on violence against children in general and online risks and threats to children in particular. Although not much is known about the actual prevalence of cyberbullying, online sexual abuse and exploitation, cyber extremism, cyber addiction and other risks and threats for children, it is evident that Indian children are being affected in many ways. As ICT and the Internet are bound to expand in the course of

India's socioeconomic development, these threats will increase because of the rapid technological evolution and the inherent vulnerability of children. There is sufficient indication of the worrying overall trends and patterns to urge for immediate action.

The online abuse and violence against children in India has to be perceived and understood within the context of violence and abuse against children in the country. ICT exacerbates the existing power relationships and pervasive violence against women and children and provides fertile ground for their misuse for harassment, abuse and exploitation. Social attitudes and norms influencing overall violence against women and children and mental health dimensions need to be understood to find ways of approaching them. There is a need to expand the data and knowledge base on online abuse and exploitation of children engaging a broader set of concerned experts in designing the enquiry as most of the studies on technology use and online violence are industry-supported and based on small samples.

There is a simultaneous need to address issues of comprehensive sexuality education with maturity and openness in order to address effectively the issues of adolescent relationships in today's times, otherwise issues such as gender violence and responsible sexual behaviour are difficult to address.

Immediate action may not be able to address every aspect of online protection of children but prioritization of action and rapid follow-through could strengthen the protective environment for children. The broad parameters of the overall strategic approach need to be agreed upon so that various stakeholders can contribute their resources and energies for a coordinated response to strengthen different aspects of the protective environment.

The challenge of creating a safe online environment for children lies in developing a range of responses that strike an appropriate balance between maximizing the potential of ICT to promote and protect children's rights and opportunities while minimizing risks and ensuring children's safety and protection. The benefits of technology and its potential to empower children, together with recognition of the resourcefulness and evolving capacity of children to take an active and responsible role in their own protection and that of others, must lie at the heart of all initiatives.

The benefits of technology and its potential to empower children, together with recognition of the resourcefulness and evolving capacity of children to take an active and responsible role in their own protection and that of others, must lie at the heart of all initiatives

Both boys and girls have a role to play and their inherent energies and potential need to be harnessed. Developing the online competencies of children must also include building their capacities and resilience as digital citizens based on values and life skills, not just be limited to avoiding the risk of specific online threats. Furthermore, schools, teachers, parents/ guardians, policymakers, industry players and other key stakeholders should adopt a proactive approach towards fostering such a favourable environment.

A public discourse on child online protection issues needs to be created to make them everyone's concern; law enforcement processes need to be activated and strengthened for the emerging and ever-evolving online challenges; and technological checks and balances need to be established and constantly updated so that systemic protection is at its best. Online diligence, monitoring and reporting against violence and related crimes need to be promoted in view of the shroud of silence around child sexual abuse, associated stigma and the hesitation in seeking help.

As a matter of urgency, a comprehensive package of specialized services should be developed for the support and recovery of child victims of online exploitation and abuse. These services should include adequate skills, capacities and resources, especially for mental health support, to meet the specific needs of child victims of online abuse. These specialized services should of course be integrated and mainstreamed in India's overall child protection systems and services.

The advantages of an enabling policy and legal framework can be realized with strong enforcement of the law and ongoing monitoring of technological developments that may require legal measures to strengthen online security

Several initiatives are underway to address the issue of child online protection in the country, each with its own scope and focus. Learning from these efforts will help to design the way forward, making documentation and sharing important aspects of the collective effort in this direction.

The existing policies and the Sustainable Development Goals 2015–2030 provide a framework for action for the Government in its efforts to protect children from offline and online abuse and exploitation. This global commitment, agreed by Heads of State and Government during the United Nation Summit in September 2015, provides for the protection of children from all forms of violence under Goal 16.2 and other related targets (5.2, 5.3, and 8.7.). This includes abuse, exploitation, trafficking, harmful practices and neglect or negligent treatment. In addition, the advantages of an enabling policy and legal framework can be realized with

strong enforcement of the law and ongoing monitoring of technological developments that may require legal measures to strengthen online security. Ensuring that systems and capacities are developed at all levels to meet these requirements is necessary.

A cohesive national response requires a multi-agency approach, strong leadership and effective coordination of the efforts of all stakeholders, each with an important and distinct role to contribute to the collective effort of building and sustaining a safe online environment for children. Who will assume this leadership role has yet to be determined. The Government's proposed establishment of a separate unit within I4C to deal with online crime against women and children, and to monitor and block child pornography/ child sex abuse images, online abuse and exploitation, may be significant. This additional unit could function as the nodal unit for coordination of the country's response to online crimes against women and children.

The obligation of protecting children from online threats is evident. Building partnerships among relevant stakeholders such as private sector actors/ICT companies, civil society organizations, academia and research organizations, mental health experts, child helplines and other reporting mechanisms, and government sectors involved in different aspects of the protective actions may be the way forward to keep professional dialogue open, sharing knowledge, experience and collective thinking for keeping pace with the demands and developing challenges in this area.

Recommendations for priority interventions

1. Leadership and partnerships for child online safety in India

- Identify key organizations and potential partnerships to lead, coordinate and monitor inter-agency efforts to ensure appropriate prevention and response to child online exploitation and abuse
- Develop a National Framework for Child Online Safety and a multi-agency action plan to be implemented through multisectoral partnerships and collaboration; including clear definitions of roles and responsibilities
- Build awareness and capacity of key partners including ICT companies, government bodies, law enforcement agencies, media, civil society actors, etc

2. Evidence, research and data on child online safety in India

- Carry out a study of the risky and harmful online behaviours of children in and out of school
- Carry out a study of the production, distribution and use of CSAM based on data available from law enforcement agencies, ICT companies, Childline India and media reports

3. Education for digital literacy, citizenship and safety

- Bring key education actors together to agree on a common action plan on digital literacy and safety
- Develop a plan to institutionalize and mainstream digital safety and literacy to reach a very large proportion of children, caregivers and relevant professionals
- Develop an age-appropriate 'Digital Safety, Literacy and Citizenship' Curriculum to be integrated and mainstreamed in the school curriculum across subjects, particularly as part of the ICT curriculum
- Ensure active and meaningful engagement of children and adolescents in protecting themselves and their peers from online abuse and exploitation
- Enable and empower parents and caregivers to play an active role in preventing and protecting children from child online abuse and exploitation

4. Legislation and policies to protect children from online abuse and exploitation

- Review and revise cyber laws related to child online abuse and exploitation
- Invest in the implementation of cyber laws and legislation via improved child-centred guidelines, structures, capacities and resources
- Develop approaches that do not criminalize children and adolescents for harmful online behaviours

5. Reporting and removing online child sexual abuse material (CSAM)

- Invest long term in an India-based Hotline able to remove high volumes of CSAM
- Establish and reinforce collaboration between the ICT industry and law enforcement actors to ensure effective reporting and removal of online CSAM
- Raise awareness of mechanisms for the reporting and removal of CSAM among children, parents and professionals
- Monitor, analyse and review data on the reporting and removal of CSAM

6. Legal investigation and prosecution of online child sexual abuse and exploitation

- Invest in the capacities and resources of the police workforce and cyber forensic professionals
- Clarify and strengthen processes and procedures for cybercrime investigations involving children
- Improve coordination and collaboration between cybercrime cells, police and ICT industry
- Apply a child-centred approach to reporting of CSAM and to the legal investigation and prosecution of child online abuse and exploitation

7. Services for child victims of the worst forms of child online abuse and exploitation

- Integrate and mainstream child online protection in existing processes and ongoing efforts to strengthen child protection systems; including defining a specific intervention package for end-to-end support for child victims of online exploitation and abuse
- Map the responsibilities and skills required by key actors (law enforcement, child protection service providers, etc.) to effectively prevent and respond to child online exploitation and abuse
- Develop a programme to strengthen capacities for child online protection across the child protection system
- Develop capacities for online counselling of child victims and child offenders involved in online abuse and exploitation (e.g., Childline India)

References

Boyd, Danah, *It's Complicated, The Social Lives of Networked Teens*, Yale University Press, London, 2014.

Gasser, Urs and Maclay, Colin M. and Palfrey, John G., 'Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations' (June 21, 2010). Berkman Center Research Publication No. 2010-7; Harvard Public Law Working Paper No. 10-36. Available at SSRN: http://ssrn.com/abstract=1628276

Government of India, Ministry of Home Affairs, National Crime Records Bureau, Crime in India Report, 2014.

Griffiths, M.,van Rooij, A., Kardefelt-Winther, D., et al., *Working towards an International consensus on criteria for assessing Internet Gaming Disorder: A critical commentary* on Petry et al. (2014), Addiction, 111, 2015.

Halder D., Jaishankar K., 'Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites', *Social Networking as a Criminal Enterprise*, edited by Marcum C. and Higgins G., CRC Press, Taylor and Francis Group, Florida, 2014.

Halder D., Jaishankar K., 'Teen Sexting: A Critical Analysis on the Criminalisation Vis-A-Vis Victimization Conundrums', *The Virtual Forum Against Cybercrime (VFAC) Review,* Korean Institute of Criminology, July/August 2014.

Holloway, D., Green, L. And Livingstone, S., 'Zero to eight. Young Children and Their Internet Use', LSE, London: *EU kids online*, 2013.

IAMAI & IMRB, *Internet in India*, November 2015. <www.iamai.in/media/details/4486>

IAMAI &KPMG, Internet on the Go. Mobile Internet - Vision 2017, July 2015. <www.iamai.in/media/details/3679>

IAMAI, Internet Readiness Index in India, February 2016. www.iamai.in/media/details/4633

IWF, Annual Report, London, 2014. <www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf>

Kardefelt-Winther, D., 'A critical account of DSM-5 criteria for Internet gaming disorder', *Addiction Research & Theory, Early Online, vol. 23, Issue 2*, 2014.

Kesavamoorthy, R., 'Legal Study on protection of Children in Social Network, special reference to India Law', I*OSR Journal of Humanities and Social Science* (IOSR-JHSS), 15(1), 2003. www.iosrjournals.org

Livingstone, S., Carr, J. and Byrne, J., 'One in Three: Internet Governance and Children's Rights', Innocenti Discussion Paper, No. 2016-01, Innocenti Research Centre, Florence, 2016.

Livingstone, S., Haddon, L., Gorzig, A., and Olafsson, K., 'Risks and safety on the Internet: The perspective of European children, Full findings', LSE, London: *EU Kids Online*, 2011.

Livingstone, S., Kirwil, L., Ponte, C. and Staksrud, E., EU Kids Online Network, 'What bothers children online?', LSE, London: *EU Kids Online*, 2013. www.eprints.lse.ac.uk/48357/

Livingstone, S., Olaffson, K., O'Neill, B. and Donoso, V., 'Towards a better Internet for Children: Findings and Recommendations' from *EU kids online* to inform the CEO coalition, LSE, London: EU Kids Online, 2012. <www.eprints.lse.ac.uk/44213>

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

Microsoft, *Global Youth Online Behaviour Survey*, 2012.

'Policies and Initiatives to Promote Children's Safe, Effective and Responsible Use of ICT', Asia Pacific Regional Consultation, Bangkok, 9-11 SeptemberADD YEAR. <http://www.unescobkk.org/ru/education/ict/current-projects/responsible-use-of-ict/policies-and-initiatives-to-promote-childrens-safe-effective-and-responsible-use-of-ict-asia-pacific-regional-consultation/>

Seth, Karnika, *Computers, Internet and New Technology Laws*, Updated Edition, Lexis Nexis, Delhi, 2013.

Seth, Karnika, *Protection of Children on Internet*, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2015.

Srivastava, A., Shinde, S., Doctor, H. & Kavadi, S. N., *Towards Digital Inclusion: Barriers to Internet Access for Economically and Socially Excluded Urban Communities*, Centre for Communication and Development Studies, Pune, 2015.

Standing Committee on Information Technology (2013-14), Fifteenth Lok Sabha, Ministry of Communications and Information Technology (Department of Electronics and Information Technology), Cybercrime, cyber security and right to privacy, 52nd Report, Delhi, February 2014.

UNESCO Asia-Pacific Regional Bureau of Education, *Fostering Digital Citizenship through Safe and Responsible Use of ICT: A review of current status in Asia and the Pacific*,APEID-ICT in Education, December 2014.

UNICEF India, Expert Consultation on Child Online Safety in India, New Delhi, 8–9 April 2016.

UNICEF India, Roundtable for the Private sector, New Delhi, New Delhi, 8 February 2016.

UNICEF, Child Safety Online, *Global Strategies and Challenges*, Innocenti Research Centre, Florence, 2011.

UNICEF, Child Safety Online, Global Strategies and Challenges. Technical Report, Innocenti Research Centre, Florence, 2012.

UNICEF, Children, ICT and Development: Capturing the potential, meeting the challenges, Innocenti Research Centre, Florence, 2013.

UNICEF, Mobile Phones. A tool for social and behavioural change. A white paper, New Delhi, 2013.

UNICEF, Mobile Phones. A tool for social and behavioural change. A working paper, New Delhi, 2013.

UNICEF, Mobile Phones. A tool for social and behavioural change. A review of case studies, New Delhi, 2013.

UNICEF, Save the Children and Global Compact, Children's Rights and Business Principles, New York, 2012.
https://www.unglobalcompact.org/docs/issues_doc/human_rights/CRBP/Childrens_Rights_and_Business_Principles.pdf

UNINOR (TELENOR), *Being Webwise, Safe Internet for Children, A National Survey Report 2014, Building online resilience among children*, New Delhi, 2014.

United Nations Office on Drugs and Crime, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, Vienna, 2015.

United Nations, Annual Report of the Special Representative of the Secretary- General on Violence against Children, A/HRC/31/20, New York, January 2016.

United Nations, Committee on the Rights of the Child, Digital Media and Children's Rights, Report of the General Discussion, New York, 2014.

United Nations, Committee on the Rights of the Child, General Comment No.12, The Right of the Child to be Heard, New York, 2009.
www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/CRC-C- GC-12.pdf.

United Nations, Committee on the Rights of the Child, General Comment No.13, The Right of the Child to Freedom, New York, 2011.
www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.13_en.pdf.

United Nations, Cyber Violence Against Women and Girls: A World-wide Wake-up Call, Report by the United Nations Broadband Commission for Digital Development Working Group on Broadband and Gender, New York, 2015.

United Nations, Realising Children's Potential and Minimizing Risks – ICTs, The Internet and Violence against Children, New York: Office of the Special Representative of the Secretary- General on Violence against Children, October 2014. <www.srsg.violenceagainstchildren.org>

United Nations, Releasing children's potential and minimizing risks. ICTs, the Internet and Violence against Children, Office of the UN Representative of the Secretary-General on Violence against Children, New York, 2014.

WePROTECT Global Alliance, 'Our Strategy to End the Sexual Exploitation of Children Online', 2016.

World Bank, Protecting Children from Cybercrime. Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying, A joint report of the World Bank and the International Centre for Missing and Exploited Children (ICMEC), Washington DC, 2015.

Zainuddin, Sivapragasam, et al., T*eleuse at the Bottom of the Pyramid: Findings from a Five-Country Study*, Colombo, Sri Lanka: LIRNEasia, November 2007.

International treaties and related documents

United Nations, Convention on the Rights of the Child, New York, 1989.

United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, New York, 2000.

United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2000.

WePROTECT Global Alliance

Indian policy and legal documents

Draft Education Policy, 2015

Indecent Representation of Women (Prohibition) Act, 1986

Indian Penal Code, 1860

Information Technology Act, 2000 and Amendment 2008, and the Information Technology (Intermediaries guidelines) Rules, 2011.

National Cyber Security Policy, 2013

Protection of Children Against Sexual Offences Act, 2012

The Constitution of India

The Goa Children's Act, 2003 and Rules 2004

The National Policy for Children, 2013

The National Policy of ICT in Schools, 2012

Key informants

The Government of India

Dr. A S Kamble, Scientist G, Senior Director, Cyber Law and E-security Group, DEITY, New Delhi

Ms. B. Bhamathi, IAS (Retd), Former Additional Secretary, MHA, Mumbai

Dr. Dinesh Paul, Director, NIPCCD, New Delhi

Mr. Kumar Alok, Joint Secretary, MHA, New Delhi

Mr. Rakesh Maheshwari, Scientist G, Director, DEITY, New Delhi

Ms. Rina Ray, Additional Secretary, School Education and Literacy, MHRD, New Delhi

Ms. Saroj Yadav, Dean, Academic and New Education Policy, NCERT

National and state level statutory bodies

Mr. Arun Mathur, Chairperson, DCPCR, New Delhi

Mr. Govind Beniwal, Former Member, RSCPCR, Jaipur, Rajasthan

Ms. Sandhya, Member, KSCPCR, Thiruvananthapuram, Kerala

Ms. Shoba Koshy, Chairperson, KSCPCR, Thiruvananthapuram, Kerala

Ms. Stuti Kacker, Chairperson, NCPCR, New Delhi

Law enforcement agencies

Mr. Mohd. Taj Hassan, Special Commissioner (Crime), Delhi Police

Mr. Navniet Sekera, IG Police, Lucknow, Uttar Pradesh

Mr. Sanjay Gautam, Deputy Superintendent of Police, CBI Training Academy, Ghaziabad, Uttar Pradesh

Ms. Seema Goel, Training Coordinator, CBI Training Academy, Ghaziabad, Uttar Pradesh

Mr. Talwant Singh, District and Sessions Judge, Karkardooma Courts, Delhi

Legal experts

Mr. Anant Kumar Asthana, Child Rights Expert and Lawyer

Ms. Aparna Bhat, Child Rights Expert and Advocate, Supreme Court, New Delhi

Dr. Debarati Halder, Cyber Expert and Honorary Managing Director, CCVC, Tamil Nadu

Ms. Karnika Seth, Cyber Law Expert and Advocate in the Supreme Court, New Delhi

Mr. Pavan Duggal, Cyber Law Expert and Advocate in the Supreme Court, New Delhi

Cyber safety experts

Mr. Rakshit Tandon, Cyber Safety Consultant

Mr. Sebastian Edassery, Director, Financial Advisory, Deloitte Touche Tohmatsu India LLP, Bengaluru, Karnataka

Corporate sector

Ms. Ankhi Das, Head of Policy, Facebook India, New Delhi

Ms. Ashima Kukreja, Head of Social Responsibility, Telenor, Gurgaon, Haryana

Ms. Chitrita Chatterjee, Associate Vice President, IAMAI, New Delhi

Mr. Deepak Maheshwari, Head, Government Affairs, Symantec, Gurgaon, Haryana

Mr. Harsha Ramchandra, Corporate Communications, TCS

Ms. Mahima Kaul, Head of Public Policy, Twitter

Mr. Nandkumar Saravade, Chief Executive Officer, DSCI, New Delhi

Ms. Patricia Cartes, Head of Global Trust and Safety Outreach, Public Policy, Twitter Inc.

Mr. Piyush Poddar, Public Policy and Government Relations Analyst, Google India Pvt. Ltd., Gurgaon, Haryana Ms. Pooja Thakran, Chief Corporate Communication Officer / Head, Corporate Responsibility, Telenor, Gurgaon, Haryana

Mr. Ravi Sharma, Executive Chairman, CMAI India, Communication, Multimedia and Infrastructure

Mr. Ritesh Mehta, Head of Economic Growth Initiatives for India and South Asia, Facebook India, New Delhi

Mr. Sanil Shirsat and Ms Saadia Memon, Intel Securities (formerly McAfee)

Mr. Shrikant Sinha, Chief Executive Officer, NASSCOM Foundation

Ms. Sonia Shrivastava, Head, Vodaphone Foundation, New Delhi

Dr. Subho Ray, President, IAMAI, New Delhi

Mr. Surjeet Singh, Deputy Manager, Social Responsibility, Telenor, Gurgaon, Haryana Ms. Susie Hargreaves, Chief Executive, Internet Watch Foundation, UK

Ms. Vineeta Dixit, Public Policy and Government Relations, Google India Pvt Ltd, Gurgaon, Haryana

Civil society organizations

Mr. Ambrish Rai, Right to Education Forum, New Delhi

Dr. Anjlee Prakash, Chairperson, Learning Links Foundation, New Delhi

Dr. Anjula Srivastava, Research Associate, Centre for Communication and Development Studies (CCDS), Pune, Maharashtra

Ms. Bharti Ali, Co-Director, Haq Centre for Child Rights, New Delhi

Mr. Bhuwan Ribhu, Activist, Bachpan Bachao Andolan, New Delhi

Ms. Hutokshi Doctor, Director and Editor, CCDS, Pune, Maharashtra

Dr. Leena Sushant, Director - Research, Breakthrough Trust, New Delhi

Ms. Nancy Thomas, Programme Manager, Tulir, Chennai, Tamil Nadu

Ms. Niharika Chopra, Project Coordinator - Legal Cell, BBA, New Delhi

Ms. Nisha Dua, Project Director, Learning Links Foundation, New Delhi

Mr. Nishit Kumar, Head, Communications and Strategic Initiatives, ChildLine India Foundation, Mumbai, Maharashtra

Ms. Raisa Anna Philip, Project Coordinator - Policy Advocacy, BBA, New Delhi

Ms. Shri. Vineet Kumar, Founder and President of Cyberpeace Foundation, India

Ms. Shobha V Iyer, Online Engagement Lead, Breakthrough Trust, New Delhi

Mr. Siddharth Pillai, Co-Director, The Aarambh India Initiative, Mumbai, Maharashtra

Ms. Sonali Khan, Country Director, Breakthrough Trust, New Delhi

Mr. Sunil Abraham, Executive Director, Centre for Internet and Society, Bengaluru, Karnataka

Ms. Uma Subramanian, Founder and Co-Director, The Aarambh India Initiative, Mumbai, Maharashtra

Ms. Vidya Reddy, Executive Director, Tulir, Chennai, Tamil Nadu

Others

Dr. Achal Bhagat, Senior Psychiatrist and Psychotherapist, New Delhi

Ms. Bindu Sharma, Asia Pacific Policy Director, International Centre for Missing and Exploited Children (ICMEC), Singapore

Dr. P.M. Nair, IPS (Retd.) and Research Coordinator and Chair Professor, Tata Institute of Social Sciences, Mumbai

Dr. Ramya Subrahmanian, Executive Director, Know Violence in Childhood Global Learning Initiative, Gurgaon

Dr. Tara, Centre for Children, Internet and Technology Distress, Uday Foundation, New Delhi

Mr. Raghav Mimani, Founder, Nischint, Dubai

UN agencies

Mr. Alisher Umarov, Chief of Education and Programme Specialist, UNESCO New Delhi Cluster Office for Bangladesh, Bhutan, India, Nepal, Maldives and Sri Lanka

Ms. Alka Malhotra, Communication for Development Specialist, UNICEF India

Ms. Clara Sommarin, Child Protection Specialist - Exploitation and Violence, UNICEF Hq, New York

Ms. Deepa Das, Education Specialist, UNICEF India

Mr. Joachim Theis, Chief, Child Protection, UNICEF India

Mr. Ramchandra Rao Begur, Education Specialist, UNICEF India

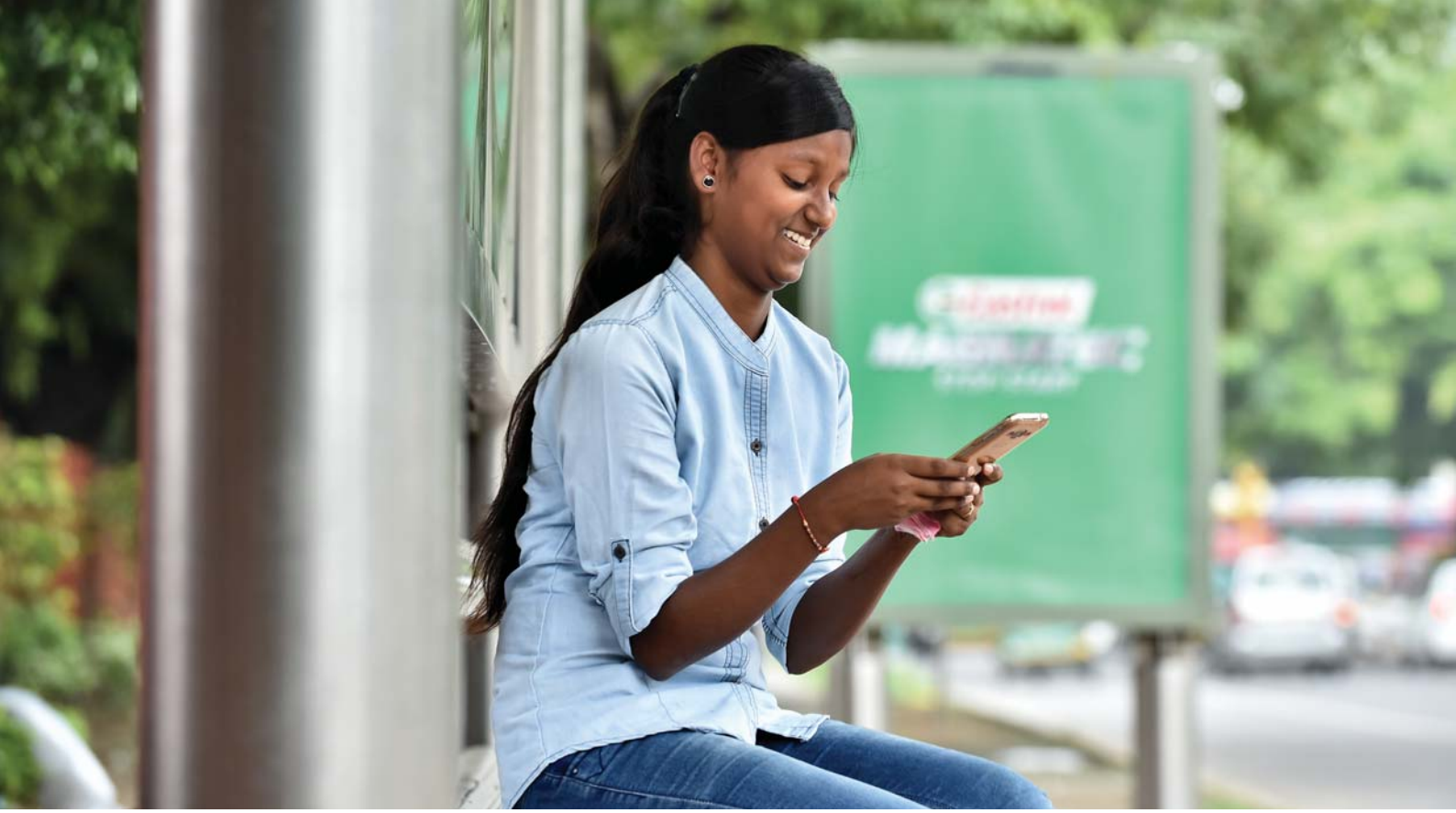
Ms. Ruchira Gujral, Corporate Engagement and CSR Specialist, UNICEF India

Dr Sandra Hernandez, Consultant, UNICEF Philippines

Ms. Serena Tommasino, Child Protection Specialist, UNICEF India

Ms. Swasti Rana, Project Officer, Anti-human Trafficking and Other Forms of Organized Crime Interventions, UNODC

Ms. Tannistha Datta, Child Protection Specialist, UNICEF India



ANNEXES

Annex 1	Indian policies and laws governing child online protection
Annex 2	National advisory on preventing and combating cybercrime against children
Annex 3	Cybercrime investigation cells in India
Annex 4	Interventions on cyber-safety in Indian states and union territories
Annex 5	Information resources available in India
Annex 6	Cybercrime investigation cells in India
Annex 7	Child online protection in India: An analysis of the national response status based on the WeProtect National model

Indian policies and laws governing child online protection

The Constitution of India guarantees Fundamental Rights to all children in the country and empowers the State to make special provisions for children (Section 1.1). The Directive Principles of State Policy guide the State in safeguarding children from abuse and ensuring that children are given opportunities to develop in a healthy manner, with freedom and dignity. The State is responsible for ensuring that childhood is protected from exploitation and moral and material abandonment.

The National Policy for Children (NPC), 2013, "affirms the Government's commitment to the rights based approach in addressing the continuing and emerging challenges in the situation of children" (Section 1.5). The State is committed to take affirmative measures – legislative, policy or otherwise – to promote and safeguard the right of all children to live and grow with equity, dignity, security and freedom, especially those marginalized or disadvantaged; to ensure that all children have equal opportunities; and that no custom, tradition, cultural or religious practice is allowed to violate or restrict or prevent children from enjoying their rights" (Section 2.2). Accordingly, the NPC seeks "to guide and inform all laws, policies, plans and programmes affecting children. All actions and initiatives of the national, state and local government in all sectors must respect and uphold the principles and provisions of this Policy" (Section 2.3).

With specific reference to education, Section 4.6 (viii) of the NPC seeks to "Ensure physical safety of the child and provide safe and secure learning environment." Section 4.6 (xi) speaks of provision of access to ICT tools for equitable, inclusive and affordable education for all children especially in remote, tribal and hard to reach areas and Section 4.6 (xii) commits to "Promote safe and enjoyable engagement of children's experiences with new technology in accordance with their age and level of maturity, even as there is respect for their own culture and roots." The provisions in the education section of the NPC emphasize safety and a safe learning environment. They emphasize use of ICT and equal access to ICTby all children. These are enabling provisions for a balanced approach to providing appropriate opportunities for accessing information, participation and building safeguards for protecting children from potential risks and harm from the online environment.

In relation to protection, Section 4.9 specifies that "The State shall protect all children from all forms of violence and abuse, harm, exploitation including sexual exploitation,

pornography, or any other activity that takes undue advantage of them, or harms their personhood or affects their development." Section 4.12 emphasizes that "The State shall ... enact progressive legislation, build a preventive and responsive child protection system, and promote effective enforcement of punitive legislative and administrative measures against all forms of child abuse and neglect to comprehensively address issues related to child protection."

Section 4.13 states that "The State shall promote and strengthen legislative, administrative and institutional redressal mechanisms at the National and State level for the protection of child rights. For local grievances, effective and accessible grievance redressal mechanisms shall be developed at the programme level."

Section 4.12 highlights a preventive and responsive child protection system and preventive measures and punitive actions against any form of exploitation and abuse. Section 4.13 refers to the access to mechanisms for redressal. In all, the protection provisions provide for a comprehensive and systemic approach to address the issue of child online protection.

Section 4.14 emphasizes that "The State has the primary responsibility to ensure that children are made aware of their rights, and provided with an enabling environment, opportunities and support to develop skills, to form aspirations and express their views in accordance with their age, level of maturity and evolving capacities, so as to enable them to be actively involved in their own development and in all matters concerning and affecting them." The emphasis on appropriate opportunities to enable children to be actively involved in their own development also implies making available equitable opportunities through ICT for their learning and empowerment and fully equipping children with the know-how to protect themselves from potential harm.

National Policy on ICT in Schools, 2012, recognized that "access to the Internet enhances the risk of inappropriate content reaching children and compromising privacy and identity of individuals. Evolving appropriate advisories for regulating access, monitoring Internet activity and education including privacy and security of students and teachers will be taken up at the instance of the Advisory Group. Heads of schools and teachers will be trained in appropriate security and regulatory measures" (Section 9.9.1).

Draft Education Policy, 2015 (School Education: Thematic area - Promotion of Information and Communication Technology systems in school and adult education): This is in the process of being developed. Broad-based consultations are underway in this regard; the proposed provisions in the draft emphasize the potential of ICT to improve the quality of education and build the capacities of teachers to develop appropriate educational content.

The draft is silent on the potential risks and harm to children from ICT, informed user behaviour and safety and protective dimensions. This is an area of advocacy with government during the process of development and finalization.

The mission, objectives and provisions of the **National Cyber Security Policy, 2013,** cover dimensions of prevention, investigation and prosecution of cybercrime, which ostensibly include cybercrime against children. Importantly, it emphasizes the need for strengthening the capacities and competencies of law enforcement agencies in view of the high level of skills and specialization required for investigating cybercrimes and collecting critical data to enable prosecution. The policy also underscores the importance of responsible user behaviour, implying users' knowledge of online risks and exercise of appropriate precautions.

This is particularly critical for children using ICT and it is the obligation of the State (Government) to create this awareness and knowledge. The provision for audit of security measures is important for quantifying the effectiveness of measures taken by various service providers for safeguarding children's use of ICT.

Section 11 focuses on enabling effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention. Section 12 emphasizes the creation of a culture of cyber security and privacy enabling responsible user behaviour and actions through an effective communication and promotion strategy.

In addition, Section D on strengthening the regulatory framework mandates appropriate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure. Under the provisions for human resource development, Section 1 seeks "To foster education and training programmes both in formal and informal sectors to support the Nation's cyber security needs and build capacity" and Section 2 stresses "the establishment of institutional mechanisms for capacity building for Law Enforcement Agencies."

The Information Technology Act, 2000, and the IT (Amendment) Act, 2008, cover the following online offences against children:

- transmission and publication of obscene material, i.e., child pornographic material or other adult content in electronic form;
- transmission or publication of sexually explicit acts in electronic formincluding any adult content video, MMS, short clip or image whether self-clicked or taken by someone else;
- publication or transmission of material depicting children in sexually explicit acts in electronic form or creating images, text, collecting, seeking, downloading, advertising, promoting or distributing content that depicts children in an obscene or sexually explicit manner;.
- enticement of a child or children into an online relationship for sexually explicit acts or in a manner that can offend a reasonable adult, or facilitate abusing children or recording in electronic form a person's own abuse or that of others relating to a sexually explicit act with children;.

- intentionally or knowingly capturing or publishing or transmitting images of a private area of any person without his or her consent including taking a picture of oneself or a person with consent and posting it on any communication device in nude or semi-nude form;
- securing access to a computer without authority, downloading or copying data (data theft), introducing a virus or causing damage to a database or programme, disrupting access, tampering with a computer in any way, charging services to another person, destroying evidence, or similar activities with the aim of causing damage;.
- dishonestly receiving any computer resource or communication device, identity theft, i.e. making use of someone's password or electronic signature, cheating by personation which could be through blogs, fake profiles, false e-mail addresses, fake images, etc.
- breach of confidentiality and privacy, i.e. sharing or making public private information.

The provisions cover child pornography, grooming, sexual predation, sex webcam recording, and live webcam streaming of sexual conduct.

Indian Penal Code: As the IT Act does not have specific provisions for offences such as criminal intimidation, hate speech, and defamatory content, the provisions of the IPC are applied in cases of online offences. These include: Section 153A (hate speech or sedition), Section 419 (cheating by personation), Section 420 (cheating), Section 500 (defamatory content), Section 506 (criminal intimidation), Section 507 (criminal intimidation by anonymous communication) and Section 292 (prohibition on possession of obscene material). The application of IPC in conjunction with the IT Act, however, can contribute to problems of interpretation and challenges the capacities of law enforcement officials and the judiciary.

Guidelines for Cybercafes under the IT Act specify identity proof, accompaniment of an adult with a child, use of commercially available safety or filtering software so as to avoid, as far as possible, access to websites relating to pornography including child pornography or obscene information. In addition cybercafes are mandated to maintain identity proof of users, user logs, and necessary documents/data for a period of one year. Cybercafes are also mandated to display a clearly visible board disallowing users from viewing pornographic sites or copying or downloading information that is prohibited under Section 6 (7) of the Rules. The cybercafes must immediately report reasonable doubt or suspicion regarding any user to the concerned police.

Mandating active supervision, monitoring and registration of cybercafes withinthe rules will make these provisions effective. In the absence of effective monitoring of cybercafes, and revocation of licenses in case of default, there is no information on effective implementation of these guidelines, the nature of breeches in procedure and resulting issues impacting child online protection in public facilities.

Guidelines for Intermediaries: The IT Act does not have explicit provisions requiring ISPs to report child pornography/child sex abuse images. Section 79 of the IT Act and Information Technology (Intermediaries Guidelines) Rules address intermediaries' liability for making available third party content. . Section 79 (1) of the IT Act protects intermediaries from liability in cases of transmission or hosting of third-party information, data, or communication links, so long as they exercise due diligence under Section 79 (2) of the IT Act and observe the Information Technology (Intermediaries Guidelines) Rules.

However, Section 79 (3) of the IT Act provides that an intermediary shall be liable for acts performed by the third party if: (a) the intermediary has conspired or abetted or aided or induced the commission of the unlawful act provided under the IT Act; or (b) the intermediary receives actual knowledge or is 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 unlawful acts, but fails to immediately remove or disable access to the materials in any manner.

In addition, the IT (Intermediaries Guidelines) Rules detail intermediaries' duties with due diligence mentioned in Section 79 (2) of the IT Act as stated below.

Section 3 (4) of IT (Intermediaries Guidelines) Rules requires intermediaries on whose computer system the information is stored or hosted or published to: 1) disable such information within 36 hours; and 2) preserve such information and associated records for at least 90 days for investigation purposes. The intermediary is required to do this upon obtaining knowledge either themselves or being informed by an affected person in writing or through an email signed with an electronic signature about any such information mentioned in Section 3 (2) of the Rules. The prescribed information includes information that: 1) is obscene or pornographic; 2) harms minors in any way; or 3) violates any law for the time being in force according to Section 3 (2) (b), (c), and (e) of the same Rules.

The IT Act contains two sections that establish data retention and preservation requirements for intermediaries, although the legal system currently only provides specific rules on data retention related to the identification of users of public computers in cybercafes and their history of website access as stated below.

Section 67C of the IT Act articulates that intermediaries shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. These Rules under Section 67C of the IT Act have yet to be promulgated by the Government.

Section 79 (2) (c) of the IT Act further provides that intermediaries are exempt from liability for third party content provided that they observe due diligence while discharging their duties under this Act and also observe such other guidelines as the Central Government may prescribe. The Information Technology (Guidelines for Cyber

Cafe) Rules were issued in exercise of powers conferred by Section 79 (2) of the IT Act in order to establish the Government's standard for what constitutes "due diligence" by an intermediary. These Rules contain provisions addressing the duties of cybercafe owners, as one of the intermediaries, to retain data as part of their duty to observe due diligence under Section 79 (2) of the IT Act.

The Protection of Children from Sexual Offences (POCSO) Act, 2012 deals with several online offences against children, including sexual harassment, grooming and pornography including:

- sexual harassment of a child by showing him or her any object in electronic form for pornographic purposes, or repeatedly making contact with a child digitally or threatening the child with use of any form of media (Section 11 (ii),(iii)&(iv)), using real or simulated images of a child for pornographic purposes or enticing children for sexual gratification or pornography as stated in Section 11 (v)&(vi) ;
- using or engaging a child in any medium such as print, electronic, computer or any other technology for preparing, producing, offering, transmitting, publishing, facilitating and distributing pornographic materials as stated in Section 13(a),(b)&(c);
- storing pornographic material in any form involving a child for commercial purposes as stated in Section 15;
- abetment to commit any of the above offences as stated in Section 16.

The media, hotels, photographic studios, clubs, hospitals, etc. are legally bound to report any child pornographic materials.

National advisory on preventing and combating cybercrime against children

F. No. 24013/07/Misc/2011-CSR.III

Government of India/ Bharat Sarkar

Ministry of Home Affairs/Grih Mantralaya

****

North Block, New Delhi.

Dated the 4th January, 2012

To,

The Chief Secretaries,

All State Governments/UT Administrations

Subject: Advisory on Preventing & Combating Cybercrime against Children.

Sir/Madam,

With the spread of computers and Internet, cybercrime has emerged as a major challenge for law enforcement agencies. The younger generations, which use the Internet and other online technologies extensively for staying connected for all day-to-day work and entertainment, including information, e-mails, social networking, e-banking, e-shopping, web-TV, news, education, home-work research, online gaming, downloading music, videos, movies and other contents, etc., are more vulnerable to targeted cyber-crime. This often happens in the form of cyber stalking, cyber bullying, child pornography, harassment, hacking of email or social networking accounts, identity theft, unwanted exposure to sexually explicit material, etc. (Brief description of the above terms is attached at Annex).

2. The following key action points have been worked out in collaboration with various stakeholders for effective prevention and combating of cybercrime against children.

   I. The Law Enforcement Agencies i.e. Police, Prosecution and Judiciary, etc. and the public at large may be made aware and trained through special training programmes/seminars and workshops for the effective implementation of Information Technology Act, 2000 read with Information Technology (Amendment) Act, 2008 and Rules made there under, as these are effective

laws to deal with cybercrime, including crime against Children. The training should be with the specific purpose of handling crimes against children.

II. Special Juvenile Police Units constituted under Section 63 of Juvenile Justice (Care and Protection of Children) Act, 2009 may be sensitized and trained to deal with children in conflict of law with respect to cyber-crimes as well.

III. Parents, teachers and children should be encouraged to play an active role by reporting suspicious behaviour and giving information regarding websites hosting exploitative images, videos and efforts to recruit or groom children for sexual abuse. Special precautions will need to be taken to monitor and regulate the spreading awareness of cybercrime among children so that it does not have any negative effect. Use of electronic and print media may also be made appropriately.

IV. It is essential to monitor and regulate social networking sites and services because it has been seen that it hosts most of the obscene materials which induce children to sexually explicit acts or other crimes. Parents, teachers and owners of the online computing facilities should be trained to implement "parental control software" in such a manner that spoofing of age, gender and identity is mitigated. In their implementation, multifactoral authentication and other security techniques should be employed.

V. Training to protect and seize digital evidence in a secure manner should be provided to law enforcement agencies and also to examiners of digital evidence.

VI. Maintaining confidentiality of the child victim and providing him/her guidance and support to deal with the after effects of such crimes should be ensured.

VII. Obtaining help and support of NGOs working in the field of online child protection.

VIII. Conducting special sensitization programmes and skill development for those manning child help lines such as 1098 or Police Control Room, etc. may be considered.

IX. On the State Police websites, social networking websites and web browsers it is suggested to have a children's corner where Internet safety tips in simple language can be explained to them and a helpline number or e-mail addresses provided, in case of any problem.

X. Efforts can be made to develop some mechanism by which online checking of registers, records of each cybercafe can be done from a central location.

XI. Mobile Internet security must be promoted among parents and children.

XII. It is often seen that processing of digital evidence in Computer Forensic Laboratories takes a long time. States must consider as take him their own central as well as regional computer forensic laboratories. Mobile Cyber

Forensic Vans would also be useful in seizing electronic evidence from the spot in a proper manner. Assistance of NASSCOM may also be taken to establish cyber labs and training. In addition to NASSCOM, help of other agencies like NTRO, CERT-In etc. may also be taken for training.

XIII. In appropriate cases, police officers may carry out undercover cyber patrol operations to identify Internet criminals, lure them by posing as minors and arrest them. The exercise should be done in accordance with Section 72 and Section 72 (A) of Information Technology Act, 2000.

XIV. Apart from legal provisions for search under Section 100 and 165 Cr. P. C., Section 80 of IT (Amendment) Act, empowering any police officer not below the rank of a Police Inspector for search, can also be used appropriately.

XV. "Cybercrime Investigation Manual" published by Data Security Council of India is a useful book and may be referred to.

XVI. Whenever it is noticed that the investigation requires information or help from outside India, CBI Interpol Division may be approached and provision of Mutual Legal Assistance Treaties and Letter of Rogatories (LRs) may be used. Ministry of Home Affairs circular No.25016/14/2007-Legal Cell, dated 31-12-2007, may be referred to for guidelines in this regard. However, it should be kept in mind that LRs are often time consuming and by the time LRs are issued, the digital footprints (evidence) is already lost. G8 24x7 Desk of CBI, which looks after network and international aspects of cybercrime, may be contacted.

XVII. Wherever any material which is covered under Section 67, Section 67 A and Section 67 (B) of Information Technology Act, 2000 and seen on the Web, which is covered under Section 69 (A) of the IT Act under 'Public Order' or 'preventing incitement to commissioning of cognizable offence' in such cases, police may consider invoking provisions of IT Procedure and Safeguards for Blocking of Information by Public Rules, 2009. Provisions of Section 67 (C) of IT Act should be used for preservation of evidence by intermediaries.

XVIII. Websites hosting online gaming or children centric content must issue specific guidelines regarding Internet safety. Those transmitting, publishing or storing obscene material in contravention to the provisions of Section 67, Section 67 (A), Section 69, Section 69 (A) and Section 69 (B) of the IT Act, must be acted against.

XIX. In appropriate cases, police should request Social Networking sites to remove undesirable contents. Most frequently visited and popular sites should be audited for security concerns. Many of these are being used either for compromising of systems or for luring and incitement of children.

3. The aforesaid measures are only indicative and the State Governments/UT Administrations may consider any additional measures for preventing & combating cybercrime against children as necessary. This Ministry may also be kept apprised of any special measures/mechanisms introduced in their respective jurisdictions so that

the same could be circulated to the other State Governments and UT Administrations for consideration/adoption.

4. The receipt of this letter may kindly be acknowledged.

Yours faithfully,

(B. Bhamathi)

Additional Secretary to the Govt. of India,

Copy for information and necessary action to:

1. The Principal Secretary/ Secretary Home – All State Governments/UT Administrations.

2. The Director General of Police – All State Governments/UT Administrations.

Definitions as per national advisory on preventing and combating cybercrime against children:

a) **Cyber stalking:** When a victim is repeatedly and persistently followed and pursued online by e-mail or other electronic communication. In such crimes Sections 66A, 66C and 66E of Information Technology Act along with Section 506, 509 IPC can be invoked depending upon the nature and facts of the case.

b) **Cyber bullying:** Acts of harassment, embarrassment, taunting, insulting or threatening behaviour towards a victim by using Internet, e-mail or other electronic communication devices. In such crimes Sections 66A, 66C and 66E along with Section 506, 509 IPC can be invoked depending upon the nature and facts of the case.

c) **Child pornography:** This has been defined in Section 67B of IT Act. Section 67 and 67A and Section 292, 293 IPC can also be invoked as per the facts of the case.

d) **Hacking of E-mails or social networking accounts:** Unauthorized use or access to e-mail or social networking accounts such as Facebook, Orkut, Gmail, Hotmail etc. Section 43 and 66C of IT Act can be invoked.

e) **Identity theft:** Has been defined in Section 66C of IT Act which can be invoked.

f) **Unwanted exposure to sexually explicit material, etc.:** When a criminal sends pictures, videos, sound clips, cartoons or animations depicting sexual content by e-mail or any other electronic means. This would include audio or video chat using web camera, etc.

    1. Section 66 A of IT Act needs to be invoked whenever any offensive, annoying or threatening email, SMS or MMS etc. is received by children who are victims of cyber bullying or stalking.

    2. Section 67 B of IT Act must be used when the electronically published or transmitted materials contain child pornographic material. The Section also prohibits grooming of children for sexual abuse, etc.

3. Section 66 A of the IT Act may be invoked whenever email or social networking accounts of a child are hacked by misusing passwords or his/her photographs, name and other unique identification feature are misused.
4. Section 66 E of IT Act can be used for violation of bodily privacy of a person.
5. Section 67 and 67 A of IT Act can be used whenever pornographic material has been received by children by email or SMS/MMS or other electronic means.

Cybercrime investigation cells in India

State/UT	Address	Contact
Andhra Pradesh/ Telangana	In Charge, Cybercrime Police Station Hyderabad City	+91-40-27852040 cybercell_hyd@hyd.appolice.gov.in http://www.hyderabadpolice.gov.in
	ACP Inspector Cybercrimes Sub-Inspector Cybercrimes IT Cell, Special Branch Cyberabad	+91-9491039167, 9491039172, 9491039088, +91-40-27853413 http://cyberabadpolice.gov.in/cybercellwebsite
Assam	Deputy Superintendent of Police CID Headquarters, Assam Police	+91-361-252618 +91-9435045242 ssp_cod@assampolice.com
Bihar	Deputy Superintendent of Police Cybercrime Investigation Unit Kotwali Police Station Patna	+91-9431818398 cciu-bih@nic.in
Delhi	Central Bureau of Investigation (Cybercrime Investigation Cell – EOU9) Plot No. 5-B, 6th Floor, CGO Complex Lodi Road, New Delhi 110 003	+91-11-24362755, 24368083 http://cbi.gov.in/speou9del@cbi.gov.in
	Assistant Commissioner of Police, Cybercrime Cell, EOW, Crime Branch 2nd Floor Police Training School,Malviya Nagar New Delhi 110 017	cbiccic@bol.net.in, dcp-eow-dl@nic.in
Gujarat	Deputy Inspector General of Police CID (Crime and Railways) 5th Floor, Police Bhavan, Sector 18 Gandhinagar 382 018	+91-79-23254384, 23250798 +91-79-2325 3917 (Fax)
Haryana	Cybercrime and Technical Investigation Cell Old S.P. Office Complex, Civil Lines Gurgaon 122 001	jtcp.ggn@hry.nic.in http://gurgaon.haryanapolice.gov.in

Jammu	Senior Superintendent of Police, Crime CPO Complex, Panjtirthi Jammu 180 004	+91-191-2578901 sspcrmjmu-jk@nic.in
Jharkhand	Inspector General of Police CID, Organized Crime Rajarani Building, Doranda Ranchi 834 002	+91-651-2400737/738 a.gupta@jharkhandpolice.gov.in
Karnataka	Cybercrime Police Station COD Headquarters, CID Annexe Building Carlton House, # 1, Palace Road Bengaluru 560 001	+91-80-22201026, 22943050 22942475; Fax: +91-80-22387611 ccps@blr.vsnl.net.in ccps@kar.nic.in cybercrimeps@ksp.gov.in http://www cyberpolicebangalore. nic.in
Kerala	Hitech Cell Police Headquarters Thiruvananthapuram 612 901	+91-471-2721547, 2722768 hitechcell@keralapolice.gov.in
Madhya Pradesh	Cybercrime Cell G 15, Police Radio Headquarters Bhadbhada Road Bhopal 462 003	+91-755-2770248 mpcyberpolice@gmail.com http:// www.mpcyberpolice.nic.in
Maharashtra	Cybercrime Investigation Cell Annex III, 1st Floor Office of the Commissioner of Police D. N. Road, Mumbai 400 001	+91-22-24691233 cybercell.mumbai@mahapolice. gov.in http://www.cybercellmumbai.gov.in
	Office of the Commissioner of Police 3rd Floor, Khalkar Lane, Court Naka Thane (W)	+91-22-25410986, 25424444 police@thanepolice.org http://thanepolice.org/cybercell.php
	Cybercrime Investigation Cell Crime Branch 4th Floor,Administrative Building No.1 Near Udyog Bhavan, Civil Lines Nagpur 440 001	+91-712–2566766 cybercell@nagpurpolice.nic.in http://www.nagpurpolice.info/ manage_pages?id=29
	Office of the Commissioner of Police 2, Sadhu Vaswani Road, Camp Pune 411 001	+91-20-020-26126296, 26122880 26208250 Fax: +91-20-26128105.crimecomp. pune@nic.in punepolice@vsnl.com www.punepolice.gov.in
Meghalaya	Superintendent of Police State Crime Records Bureau Shillong	+91-9863064997 scrb-meg@nic.in http://meghpol.nic.in

Odisha	Cybercrime Police Station Criminal Investigation DepartmentCrime Branch Cuttack 753 001	+91-671-2305485 sp1cidcb.orpol@nic.in
Punjab	DSP Cybercrime Cybercrime Police Station S.A.S Nagar Patiala	+91-172-2748100
Rajasthan		+91-9672700012 cyber@cybercellindia.com; http://www.cybercellindia.com
Tamil Nadu	A-Wing, 3rd Floor, Rajaji Bhavan Besant Nagar Chennai 600 090	+91-44-24461959, 24468889, 24463888 hobeochn@cbi.gov.in
	SIDCO Electronics Complex Block No. 3, 1st Floor Guindy Industrial Estate Chennai 600 032	+91-44-22502526 spcybercbcid.tnpol@nic.in; http://cbcid.tn.nic.in
	Assistant Commissioner of Police Cybercrimes Cell Vepery Chennai 600 007	+91-44-23452348, 23452350 cybercrimechn@yahoo.com
Uttarakhand	Sub Inspector of Police Special Task Force Office Dehradun	+91-135-2640982 +91-9412370272 dgc-police-us@nic.in
Uttar Pradesh	Cyber Complaints Redressal Cell Nodal Officer Cybercrime Unit, Agra Range 7,Kutchery Road, Baluganj Agra 232 001	+91-562-2463343 Fax: +91-562-2261000 info@cybercellagra.com digraga@up.nic.in http://www.cybercellagra.com
West Bengal	DIG CID Cyber Cell Bhawani Bhawan, 3rd Floor, Alipore Kolkata 700 027	+91-33-24506100 Fax: +91-33-24506174 occyber@cidwestbengal.gov.in mail@cidwestbengal.gov.in http://cidwestbengal.gov.in

http://infosecawareness.in/cyber-crime-cells-in-india and http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html

Annex 4

Interventions on cyber-safety in Indian States and Union Territories

- This is not an exhaustive list of initiatives.

State/UT	Initiatives
Assam http://www.cyberfocus.in http://hb.cyberfocus.in	Cyber Focus is an NGO that was founded in 2014, Through its Happy Browsing project it organizes seminars in schools, colleges and offices to raise public awareness of cyber safety and security related issue
Madhya Pradesh http://prts-mppolice.nic.in/black-ribbon-initiative.html	The Police Radio Training School, Indore, has developed the Black Ribbon Initiative, an extensive awareness and public outreach programme to promote public awareness and alertness about computer security. It is designed to protect people from becoming either victims or perpetrators of cyber offences under the various sections of the IT Act (Amended), 2008, due to ignorance or deliberate misdeeds.
Maharashtra http://cybersafeindia.org/index.html	Cyber Safe India works to ensure cyber space is secure and safe for netizens of India., The organization facilitates and organizes multiple nationwide awareness programmes, workshops, and awareness trainings in association with supporting bodies from the central government, state police organizations, International Cyber Security Protection Alliance (ICSPA), National Cyber Security Alliance (NCSA), Computer Society of India, National Security Database (NSD) and Internet Safety Society (ISS). They assist parents, schools, teachers, citizens on cyber safety education
Gujarat http://cskgujarat.gov.in/	Cyber Suraksha Kavach aims to secure the state and citizens of Gujarat against cyber adversaries by building much needed cyber resilience for citizens, businesses and other organizations in the state of Gujarat. Cyber Suraksha Kavach develops and promotes a culture of cyber security and safer Internet usage practices to make people, especially children and other gullible users, aware of fundamental DOs and DON'Ts.
Kerala http://discfoundation.com/	The Developing Internet Safe Community (DISC) Foundation comprises a team of global experts on child protection online. It was formed to address potential threats and vulnerabilities posed to Internet users and to facilitate creation of a safer online environment by building awareness of cyber-crimes amongst adults, teenagers and children. DISC engages with experts to develop technical, legal and educational solutions bridging knowledge gaps and creating suitable interventions.

Mizoram http://www.aizawl.nielit.gov.in/new2/projects-services/cyber-security-awareness-project/	Department of Information Technology has identified' Creating mass cyber security awareness among schools, colleges and government employees through appropriate training and campaign mechanism in North-Eastern States of Mizoram, Nagaland and Tripura' as a critical area for intervention. The project aims to address gaps in cyber security awareness, particularly in the North-Eastern region of the country. It proposes development of standard modules and materials on cyber security awareness in local languages for participating states which would then be and disseminated to school and college students and government departments through NIELIT in North-Eastern states of Nagaland, Mizoram and Tripura.
Uttar Pradesh http://theladiesfinger.com/ups-1090-womens-helpline-seems-impressive-but-should-we-be-skeptical/ https://uppolice.gov.in/page.aspx?women-power-line&cd=MQAzADIAMAA per cent 3d	Uttar Pradesh police has set up 1090, The Women Power Line, a helpline for women and girls to register complaints of phone harassment, and more recently, other forms of sexual harassment. The helpline is manned by 'Power Angels' and the initiative is meant to 'foster a police-citizen partnership to create safer public spaces for women.'
West Bengal http://wwwkolkatapolice.gov.in/ComputerandInternet.aspx http://indiablooms.com/ibns_new/news-details/N/11760/west-bengal-police-in-it-hub-releases-cyber-security-booklet.html	Kolkata police has set up a website with a whole section on computer related offences and safety measures and also produced a booklet on cyber security.

Annex 5

Information resources available in India

Website	Content
www.indianchild.com	Indian Child provides parents with information to keep their children safe online. It offers a guide to Internet safety, the use of software to prevent/control online threats and reporting of inappropriate or illegal content. In addition, it lists sites that it deems to be safe for children to use, as well as an Internet safety pledge for children to sign.
www.naavi.org	Naavi.org focuses on laws to address cybercrime. It provides information about cases in India that involve Internet and related technologies and also links with Internet safety information
www.childprotectionindia.com A social initiative of Foundation for Institutional Reform & Education (FIRE), NGO	Childprotectionindia.com spreads public awareness about threats children face online such as cyber bullying, cyber grooming, cyber stalking, Internet addiction, cyber pornography and Indian laws for child protection. Also offers legal advice and counselling support for the children involved in cybercrimes. It offers preliminary guidance to safeguard children from cybercrime and to protect their privacy. The website contains useful cyberlaw resources on subjects of protection of children on the Internet, cyber wellness and netiquette for children and parents.
www.aarambhindia.org	Channelizes the work, information and discussions on child sexual abuse and exploitation in the larger context of child protection in India and around the world. It also has a separate section on online safety for children with videos and several resources.
http://www.netsafety.nic.in/ This site is operated by the National Informatics Centre (NIC) of the Government of India, which focuses primarily on e-Governance.	Educates concerned parents about the risks of online pornography and provides basic advice on warning signs that a child might be accessing inappropriate content, as well as advice on how to protect children. It also provides links to enable parents to contact their nearest police station, should they need to report illegal content.

www.tulircphcsa.org	Tulir - Centre for the Prevention and Healing of Child Sexual Abuse (CPHCSA) works on prevention of child sexual abuse, including online sexual abuse and exploitation through the concept of personal safety education. It provides proactive and timely support to abused children and works holistically to empower them to overcome abuse and regain normalcy with family and community.
www. cyberpeacefoundation.org	Cyberpeace Foundation focuses on raising awareness, counseling, educating, training and reach out to the citizens, governments, law enforcement agencies, private enterprises, NGOs working on cyber crimes and cyber security experts to provide a common platform to tackle cyber-crime
www.infosecawareness.in	The Information Security Education and Awareness (ISEA) Project of Department of Electronics and Information Technology generates information security awareness amongst children, home users and non-IT professionals. The site provides detailed guidelines on Internet ethics, chatting, e-mails, social networking, passwords etc. and also explains risks of various online activities
www.asianlaws.org/ fact/index.htm	Freedom from Abuse of Children through Technology (FACT) focuses on online risks to children, reasons for concern, guidelines for parents and tips for children.
https://cybermumindia. wordpress.com	Cybermum India is Intel Security's initiative in which Anindita blogs about the dangers children face online as well as shares her ideas for steering clear of them on Facebook and Twitter. As part of the campaign to educate parents, teachers and children on this topic, Anindita also conducts informative sessions in schools.
www.ccvc.org	Centre for Cyber Victim Counselling works for te victims of cybercrime in India, educating people on the nature of the crime that has been committed, providing help to take action against the offender, counselling individuals to recover from the trauma of the offence, providing guidance to understand the legal scenario and how to reach the police, if police assistance is required. The organization is Several resources and articles are available on cyber offences against children.
Cybersafe India Alliance **http://cybersafeindia.org/ cyber-safety-kids.html**	CyberSafe India Alliance spreads nationwide awareness on new age technological crimes and frauds and safeguards people. It facilitates and organizes awareness programmes, workshops and awareness trainings in association with supporting bodies from the Government of India, state police organizations, International Cyber Security Protection Alliance (ICSPA), National Cyber Security Alliance (NCSA), Computer Society of India, National Security Database (NSD) and Internet Safety Society (ISS).Cyber Safe helps parents to understand their role and responsibility in guiding their children towards

www.tulircphcsa.org	a safer cyber world; advises parents on how to help their children should one of them become involved in a cyber crime; provides information for students about cyber crimes and how to use Internet wisely; trains the authorities on how to check the contents used by students in school; and organizes public awareness programmes on online safety and security.
Jaago Teens **www.jaagoteens.com**	Jaago Teens spreads awareness of safe and responsible Internet usage amongst school children. Its slogan is "Beware, Be aware and Be Web Aware". It sensitizes students, teachers and parents through workshops in Delhi schools and has raised awareness and built competence among children on safe access to the Internet. The workshops provide step-by-step education for correct, safe and optimum usage of the Web, including the concepts of virtual world versus real world; searching for authentic information; proper e-mail and blog usage; netiquette and scruples to be observed; staying away from inappropriate content; and encouraging safe and optimum usage to benefit from the Net.
Jaago Teens **www.jaagoteens.com**	Jaago Teens spreads awareness of safe and responsible Internet usage amongst school children. Its slogan is "Beware, Be aware and Be Web Aware". It sensitizes students, teachers and parents through workshops in Delhi schools and has raised awareness and built competence among children on safe access to the Internet. The workshops provide step-by-step education for correct, safe and optimum usage of the Web, including the concepts of virtual world versus real world; searching for authentic information; proper e-mail and blog usage; netiquette and scruples to be observed; staying away from inappropriate content; and encouraging safe and optimum usage to benefit from the Net.
Learning Links Foundation	Learning Links Foundation, a not for profit, is dedicated to "Empowering Lives". Working in the Formal and Non-formal Education sector, the Foundation has four domains of specialization; enhancing the Quality of Education, strengthening Citizenship, harnessing the power of Technology for Educational and Social Improvement and supporting Sustainable Social Innovation
Technical solutions	
McAfee Total Protection Family Protection?	Intel Securities launched this parental control programme to protect children of all ages from online risks while allowing them the freedom to safely explore the Internet. It enables parents to gain better insight into the digital lifestyles of their children. Parents can choose to block categories of sites, filter out only a handful of sites, or block nothing at all and simply review online activity reports. Its innovative features such as online activity reports, age appropriate settings, and YouTube, games and website blocking provide Indian parents with a powerful tool to ensure their children stay safe when using the Internet.

Nischint Solutions	This is a children's safety mobile app which runs on Android, iOS and Windows operating systems. It helps parents safeguard children by screening out hazards posed by the digital world. The mobile app incorporates digital tools to monitor phone calls, SMS, apps, websites, images and videos, schedule app usage and time, track location and sets up GPS safe zones, monitors Facebook posts, and provides emergency services like child SOS buttons.
International websites	
www.icmec.org	The International Centre for Missing and Exploited Children (ICMEC)identifies gaps in the global community's ability to protect children from abduction, sexual abuse and exploitation, and assembles the people, resources and tools needed to solve those problems. ICMEC focuses on programmes that address the complex issues surrounding missing children, child abduction, child sexual abuse, child sexual exploitation and offers support to governments, policymakers, law enforcement, prosecutors, industry, civil society, and others across the globe. ICMEC also advocates for changes in laws, treaties and systems to protect children worldwide. Several resources are available on the site.
www.lse.ac.uk/media@lse/research/Global-Kids-Online.aspx	This is an international research project which has been launched by the London School of Economics (LSE), UNICEF Office of Research and EU Kids Online to develop a global research toolkit, building on the one developed by EU Kids Online, as a flexible resource for researchers around the world gathering evidence on children's online risks, opportunities and rights.
www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx	EU Kids Online is a multinational research network that enhances knowledge of European children's online opportunities, risks and safety. It uses multiple methods to map children's and parents' experience of the Internet, in dialogue with national and European policy stakeholders.
www.fosi.org	Family Online Safety Institute (FOSI) brings together and highlights the best safety messages, tools and methods to reach parents, children and caregivers together with efforts to educate and inform governments, regulators, industry and media around the world on a balanced approach to online safety. FOSI's Good Digital Parenting provides videos, tip sheets, resources, blogs, and more.
www.ceop.police.uk	The National Crime Agency's the Child Exploitation and Online Protection Command (NCA's CEOP) works to identify the main threats to children and coordinates activity against these threats to bring offenders to account in collaboration with child protection partners across the UK and overseas. It protects children from harm online and offline, directly through NCA led operations and in partnership with local and international agencies.

www.ecpat.net/what-we-do	ECPAT International is a global network of organizations working for the elimination of child prostitution, child pornography and the trafficking of children for sexual purposes. It seeks to ensure that children everywhere enjoy their fundamental rights free and secure from all forms of commercial sexual exploitation.
www.gov.uk/government/publications/weprotect-summit-2015-in-abu-dhabi-supporting-documents	#WePROTECT Children Online Summits of 2014 and 2015 accelerated global action to deter, disrupt and detect pedophiles using the Internet to commit their crimes. Outcome of these summits include statements of action and a model national response for preventing and fighting child sexual exploitation and abuse. Forty-four countries, civil society organizations, international organizations and industries have signed the statements of action to globally fight online child sexual exploitation.
www.digitalcitizenship.net	Digital Citizenship helps teachers, technology leaders and parents to understand what students/children/technology users should know to use technology appropriately. Digital Citizenship prepares students/technology users for a digital society by establishing the norms of appropriate, responsible technology use.

Cybercrime investigation cells in India

Title	Company	Year	Key findings	Key findings	Title
Webwise A National Survey Report 2014 **'Building online resilience among children'**	Telenor (formerly Uninor)	2014	**Online activities of children** Children engage themselves in a range of online activities, researching for school projects, social networking, especially on Facebook, downloading music and films, playing online games **Online safety:** About 43 per cent of the students inherently believed that they had the ability to protect themselves on the Internet. Their number increased to 74 per cent after the workshop. Only 16 per cent thought that they were incapable of protecting themselves online. **Passwords**: Fifty-five per cent of the children admitted to having one or more common passwords for various accounts, probably unaware that not using different passwords poses the security risk of the account being	The survey was conducted alongside the Webwise workshops. **Objective**:To identify the level of awareness and understanding of school children on issues like cyber bullying and their ability to safeguard themselves against online threats. In addition, to study changes in behaviour and attitudes of the students attending Telenor's Webwise workshops.	https://www.telenor.in/public/pdf/uninor_CR_web.pdf

			hacked. Forty-five per cent children used passwords that were unique to each account; these may or may not have been strong passwords. **Privacy settings**: Forty-six per cent of the children felt that their privacy settings were safe enough but their percentage declined to 40 per cent after the workshop. In contrast, the percentage of children considering their privacy settings unsafe increased after the session. Most children (84 per cent) felt that it is not safe to chat with strangers online, which contradicted their propensity to link unknown people to their Facebook profiles. **Online threats**: Thirty per cent of the children acknowledged that they had been virtually harmed. About half of them had received demeaning or indecent messages. Seven per cent had been humiliated by public uploads of their photos and videos, 7 per cent had discovered that certain lies and rumors had been spread about them online, and another 6 per cent said their private information had been shared online without their permission.		
Teens, Tweens and Technology Survey	Intel Security	2015			

			• 77 per cent created their Facebook account before the age of 13 years. Of those active on social media: • 69 per cent published photos • 58 per cent posted their email address • 49 per cent posted the name of their school • 46 per cent posted their birth date and 42 per cent shared their phone number • 82 per cent were concerned about maintaining privacy of their personal information • 44 per cent would meet or had met someone in person after meeting online **Parents:** Forty-eight per cent parents believed the worst thing that could happen to their children was interacting with strangers online. This belief did not translate into remedial action. About 17 per cent of parents were interested in finding out if their children were interacting with strangers online. **Discussions between parents and children** Ninety-one per cent of parents claimed to have had a discussion with their children about the risks of social media although interacting with strangers was not one of the primary topics. The following were the most discussed topics:	India and survey the concerns of parents.	http://intelsecurityapac.com/digitalsafety/wp-content/uploads/sites/40/2015/10/Intel-Security_India_Press-Release_TeensTweensTech_271015.pdf

			• Cyber criminals and identity theft – 71 per cent • Privacy settings – 62 per cent • Cyber bullying – 57 per cent • Online reputation – 53 per cent • Popularity among friends – 52 per cent		
Teens, Tweens and Technology Survey	McAfee (Intel Securities)	2015	**Ownership and usage:** Eighty per cent of children who took part in the survey owned personal computers, 69 per cent owned mobile phones, and 19 per cent used multiple devices to access the Internet **Online habits:** Sixty-two per cent of all polled children shared personal information online and 58 per cent had also shared their home addresses. About 39 per cent did not tell their parents about their online activities. **Online experiences:** Twelve per cent had been victims of some kind of cyber threat.	Synovate, the market research arm of Aegis Group Plc, conducted the survey. **Objective:** To study online safety of children **Sample:** The survey covered 500 children and 496 parents in 10 cities (New Delhi, Mumbai, Pune, Ludhiana, Kolkata, Ahmedabad, Bangalore, Chennai, Hyderabad, and Cochin).	http://intelsecurityapac.com / digitalsafety/2015/10/27/research-india-ttt/
GenY Survey	TCS	2014-15	**Ownership and usage:** Seventy-two per cent owned smartphones, the most preferred gadget for 4 out of 10 surveyed. **Access to Internet:** Fifty-five per cent through desktop and laptops and 30 per cent through smartphones	**Objective:** To capture the trends, pulse and adaptation of school students from class 8–12 to changing digital technology, and to comprehend and compare the differences between school students in the major metros and mini metros of India.	http://www.tcs.com/SiteCollectionDocuments/TCS-GenY-Survey-2014-15.pdf

			Online habits • 30 per cent responded to notifications within 5 minutes; 40 per cent responded once a day; 76 per cent spent an average of 60 minutes on social media every day • 29 per cent wrote posts; 25 per cent chatted; 14 per cent posted photos; 46 per cent used FaceTime, Skype, Google Hangout • WhatsApp was by far the most popular instant messaging platform (58 per cent) followed by SMS (20 per cent). • Face-to-face or in-person communication remained the most preferred way of communication with friends (36 per cent), though 46 per cent said they digitally stayed in touch using video chat. **Social media** was not used for studies although considered useful for keeping in touch with friends and family and staying abreast with current affairs but not for studies although 7 of 10 said it made them more aware of current events and helped them keep in touch with friends and family. **Online learning** • Wikipedia – 63 per cent • PDFs –51 per cent • Online videos– 44 per cent	**Sample:** The survey covered 12,365 students in the age group of 12–18 years from 1,739 schools across 14 Indian cities - Ahmedabad, Bangalore, Bhubaneswar, Chennai, Coimbatore, Delhi, Hyderabad, Indore, Kochi, Kolkata, Lucknow, Mumbai, Nagpur and Pune. **Time period:** July–November 2014, during the nationwide TCS IT Wiz programme **Primary data collection:** Questionnaires at each of the locations	

			Main sources of news • TV and newspapers – 76 per cent • Online sources – 53 per cent • Links from friends and family – 36 per cent **Social networking preferences** • 9 out of 10 had Facebook accounts; 52 per cent were part of at least one community on Facebook. • Google+ (65 per cent); WhatsApp (6 of 10); Twitter • Sports personalities (66 per cent), celebrities (55 per cent) and film stars (54 per cent) were the most followed. **Shopping and e-commerce:** Two thirds shopped online primarily for gadgets. Top items bought were: electronics (66 per cent), books (61 per cent); movies (41 per cent); travel (39 per cent); and clothes (36 per cent). There were not many variations in choices or usage patterns when it came to gender of the student. **Parental controls:** Fifty-two per cent of the respondents said their online activities were monitored by parents. More than half of those, whose parents monitored their online activities, gave password access to online accounts.		

			Career interests: IT and engineering were the most sought after career options, especially among the boys (59 per cent each) and girls: (42 per cent each).		
Norton Cyber Security Insights Report	Norton by Symantec	2015			https://us.norton.com/norton-cybersecurity-insights-report-india
GenY Survey	TCS	2013-14	Mini metro teenagers led metros in adopting digital lifestyles **Social trends** • Facebook was the most preferred social networking playground; 76 per cent had an account (it was 86 per cent in 2012) • 48 per cent of urban teenagers posted on Facebook once in every three days • 53 per cent of high school students had more than 120 friends, whereas 60 per cent had over 120 friends in mini metros. • Google+ was becoming popular, Orkut was history. Twitter is complex, therefore not popular. • 87 per cent of high school students thought social media had made them aware of current affairs **Gadgets and net surfing habits:** 9 out of 10 urban teenagers had phones. Tablets were as popular as mobile phones	**Sample:** The survey covered 18,196high school students in the 12–18 year age group across 14 Indian cities - Ahmedabad, Bangalore, Bhubaneswar, Chennai, Coimbatore, Delhi, Hyderabad, Indore, Kochi, Kolkata, Lucknow, Mumbai, Nagpur and Pune. **Time period:** July–December 2013 **Primary data collection:** Questionnaire at each of the locations	

			both in metro and mini metros. Cybercafes were barely used in the metros. **Online trends:** 7 out of 10 urban teenagers shopped online They had moved from buying movie tickets to high value items		
GenY Survey	TCS	2012	In smartphone usage youth from Tier-II cities overtook metro youths. **Ownership and usage:** • Own mobile phones – 7 out of 10 students • Use mobile phones to access Internet – 20 per cent (compared to 12 per cent in 2009) • Use Facebook – 92 per cent • Online purchase of movie tickets – 62 per cent • Online purchase of books, DVDs and music – 47 per cent	TCS IT Wiz, India's biggest IT quiz for schools, started in 1999 as an educational initiative for students of classes 8–12. Approximately 17,000 students across India participated in the TCS IT WIZ, which is a nationwide study that could capture the trends and pulse of the youth across this nation with regard to technology. Sample: There were 17,478 Indian high school students of 12–18 year age group who participated in 12 cities Time period: August–December 2012	

#WePROTECT Children Online

Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response

Annex 7

Child online protection in India: An analysis of the national response status based on the WeProtect national model

Capability	Attribute	Best Practices	Current Capabilities	Constraints	Required Actions
Policy and Governance	**1) Leadership**	An accountable committee for national governance and oversight	• Legislature: Political interest was demonstrated via Parliamentary Standing Committee on Information Technology (2013-14) Cybercrime, cyber security and right to privacy, 52nd Report, February 2014. • Executive: While MHA has been responding to cybercrime and online threats, no nodalleadership role being played through a coordination committee which could bring together all Government stakeholders.The proposed National Cybercrime Coordination Centre, I4C unit is expected to have a separate unit dealing with women and children which may play the nodal role. • Judiciary: Recent Supreme Court directive to government on addressing child pornography urgently indicates proactive concern.	• A cohesive national response has yet to be developed. • Focus on national security and financial fraud. • Clarity on the role of the proposed I4C unit in online protection of children and women is needed. • Inadequate public and bureaucratic awareness of child online threats contribute to vulnerability of children.	• Clear Government directions for comprehensive Child Online Protection (COP) is required

	2) Research, Analysis and Monitoring	National situational analysis of CSEA risk and response to establish a baseline and indicators for measurements	• Inadequate data and evidence on COP issues • Surveys of the usage pattern and outreach of digital technologies and internet have been done mostly by the ICT industry. • Little information on the social impact on children. No comprehensive analysis of the experience of children and parents. • Considerable anecdotal information from motivated professionals, civil society organizations	• The understanding of the patterns of use of ICTs, prevalence of child online threats and their impact on children is incomplete and inadequate. • Academics, public health and child protection professionals have not begun to engageseriously in research on this issue.	• Sound evidence on children's safety and exposure to online risks is needed to inform law, policy, prevention and response initiatives for COP.
	3) Legislation	Comprehensive and effective legal framework to investigate offenders and ensure protection for victims	• Adequate, if not comprehensive, legal framework for investigating most online offences against children. • Implementation challenges due to capacity deficits, inadequately equipped investigating machinery, poor securing of evidence and weak prosecution. • Weak law enforcement • Lack of cohesive approach is reflected in inadequate services and protection of victims • Review of amendments required to IT Act isunderway	• Insufficient knowledge and skills within systems and service providers constrain effective implementation of the existing laws. • Insufficient monitoring and analysis of reasons for ineffective enforcement of laws feeding into implementation.	• All online offences against children with a universally accepted terminology need to be addressed by strengthening legislation. • Scope for strengthening the framework to align it fully with CRC and international standards.

Criminal Justice	**4) Dedicated Law Enforcement**	National remit; trained officers; proactive and reactive investigations; victim-focused; international cooperation	• Training of investigating officers inadequate. • A large scale training initiative in cybercrime investigation by MHA in final stages of clearance for implementation. • Investigations of online offences against children hampered by inadequate forensic capacities and facilities leading to low prosecution rates.	• Investigations continue to be hampered by too few cyber forensics centres and skilled human resources. • International cooperation is either not forthcoming, slow or hampered by lack of mutual agreements.	• Develop and deploy specialization in cyber skills and forensic facilities to strengthen investigation and law enforcement.
	5) Judiciary and Prosecutors	Trained; victim-focused	• Few cases reach the courts. Convictions are difficult due to lack of or poor evidence. And the justice system is not orientated sufficiently to the nuances of online offences against children and the rights of affected children.	• Inadequate orientation to cybercrime in general and cyber offences against children in particular.	• Knowledge, skills, systems and tools enable the Judiciary and prosecutors to perform victim-focused investigations and secure positive judicial outcomes.
	6) Offender Management Process	Prevent re-offending of those in the criminal justice system nationally and internationally	• No interventions.	• Children and young people who commit an offence unwittingly or deliberately without the knowledge of the gravity and consequences of their actions are at risk of being dealt with by the law enforcement system without receiving counselling and other support.	

	7) Access to Image Databases	National database; link to Interpol database (ICSE)	• Technologies are available to law enforcement agencies. Government is also willing to invest in appropriate technology.	• A national image database which can complement global images databases has not been developed. • Lack of protection of Indian children from potential abuse and exploitation	• Speedy removal of CSAM limits their further spread and contributes to protection of Indian children from online abuse and exploitation.
Victim	**8) Victim End to end support**	Integrated services provided during investigation, prosecution and after-care	• Comprehensive support services for child victims of online exploitation not developed. • Inadequate information on financial and human resources invested for child online protection by various stakeholders. • Scope for strengthening the framework to align it fully with CRC and international standards.	• Few professionalvictim counselling services available with limited reach. • Professionals working with and for children not adequately equipped to deal with all aspects of child online protection.	• Appropriate support services for child victims required during investigation, prosecution and after care to avoid the risk of re-victimization and to benefit from effective recovery and reintegration.
	9) Child Protection Workforce	Trained, coordinated and available to provide victim support	• The Integrated Child Protection Scheme provides the space and outreach for capacity development of staff to provide victim support services. • Online threats and services for victims not part of capacity development of ICPS functionaries, CWCs and JJBs • NIPCCD willing to incorporate management of online threats in 2016 review of training modules for ICPS functionaries at all levels	• Main protection services infrastructure not equipped adequately to provide appropriate support services to victims of child online exploitation.	• Children have access to services that support them through the investigation and prosecution of online crimes against them.They have access to specialised psychological services; and rehabilitation, repatriation and resocialization services.

	10) Compensation remedies and complaints arrangements	Accessible procedures	• Procedures not known or complicated. They need to be made more accessible. • Channels for complaints and seeking remedies not advertised or known by concerned people.	• Victims not receiving mandated compensation and remedies as a right.	• Unhindered access to remedies and compensation for all child victims of online exploitation.
	11) Child Helpline	Victim reporting and support; referrals to services for ongoing assistance	• Childline, a toll free helpline operates in 366 cities/districts in 34 States/ UTs through its network of over 700 partner organizations across India. It has plans to expand to 600 cities with a network of 3000 partners. • Childline has begun receiving distress calls related to online abuse from children. But these are not being quantified and analysed as a routine yet.	• Childline not fully equipped and supported to respond to the assistance requirements of victims of online threats. • Inadequate orientation to handle such calls and difficulties in referral to appropriate services for ongoing help.	• Increased victim reporting and support with referrals to services for ongoing assistance.
Societal	**12) CSEA Hotline**	Public and industry reporting for CSEA offences (online and offline); link to law enforcement and child protection systems	• Police Cyber Cells are only reporting facility. • Knowledge of industry reporting protocols not widespread.	• Inadequately publicised reporting mechanisms. • Overall ignorance of where and how to report online threats to children and seek redress which needs to be remedied.	• Enhanced reporting of online exploitation of children by industry and the public.

	13) Education Programme	For: children and young people; parents and carers; teachers; practitioners; faith leaders	• Awareness and education are widely accepted as an important preventive measure.Several civil society, industry and government initiatives support safe online etiquette for children. Motivated individuals are also involved in awareness programmes for children and parents. However, awareness programmes for children and young people not system-wide.	• No unified approach towards awareness creation and digital citizenship initiatives • The approach to informing and educating children and young people has been piecemeal and neglects rural and semi-urban areas. • Critical mass stakeholders not reached with essential information on prevention and responsible use.	• All sectors and stakeholders understand and develop a coordinated approach for equipping children, parents teachers and public with skills for safeguarding against online threats and being responsible digital citizens
	14) Child Participation	Children and young people have a voice in the development of policy and practice	• Several social responsibility initiatives of the ICT and internet companies engage with children and young people.	• Outreach is extremely limited.	• The resourcefulness and evolving capacity of children to take an active role in their own protection and that of others, is fully exploited in initiatives engaging children and building digital citizenship. • Messages adapted for children creatively with their insights.
	15) Offender Support Systems	Offender Support Systems:	• Not existent.		

Industry	**16) Notice and Takedown Procedures**	Local removal and blocking of online CSEA content	• Self-regulation and notice and takedown system for CSAM by the ISPs. • Different social media platforms have their own system and protocols for notice and removal of objectionable content.	• Less known/ inadequate reporting environment/ systems. • Grievance reporting facilities not well-known nor prominently displayed on websites.	• The public can proactively report CSEA offences with the industry having the power, willingness and mechanisms for blocking and removing online CSAM and proactively addressing local issues.
	17) CSEA Reporting	Statutory protections that allow industry to effectively and fully report CSEA, including transmission of content, to law enforcement or other designated agency	• Industry members have their own systems/protocols for reporting the transmission of content, law infringements to law enforcement agency and providing evidence for prosecution. • MHA reports slow response to requests for evidence based on servers being outside India and Indian law not being applicable.	• System seems to work for local complaints but there are reservations for complying to requests concerning materials that are originating abroad.	• Build Industry understanding and capacities on CSEA and online protection using global frameworks and guidelines • Develop processes for handling child sexual abuse content. • Develop safer and age appropriate online environments.

	18) Innovative Solution Development	Industry engagement to help address local CSEA issues	• Industry involved in awareness initiatives for children and parents	• Individual efforts by industry based on their own global agenda and priorities. However, a coordinated industry response to agreed-upon priorities is lacking.	• Cohesive industry response to solution finding based on nationally identified priorities.
	19) Corporate Social Responsibility	Effective child-focused programme	• Companies have their own agenda, not necessarily aligned to a local consensus-driven agenda for action. • No common platform for sharing information and reports of actions on a periodic basis.	• Difficulties in harmonizing CSR priorities with social policy and civil society engagement. • No significant partnerships towards common cause.	• ICT industry proactively engaged in finding solutions to the local prioritised problem of child online exploitation.
Media and Coms	**20) Ethical and informed media reporting**	Enable awareness and accurate understanding of problem	• Media has shown its openness to explore and report on issues concerning children and technology use.Most of the information on social media, internet and cybercrime and exploitation of children in the public domain are media reports. However, the content needs to be scrutinized for veracity and ethics in reporting.	• Sporadic reporting on child online threats without any strategic planning for creating a public awareness of issues and redressal options.	• Informed and strategic communication can promote public awareness and understanding of COP.
	21) Universal terminology	Guidelines and application	• No guidelines have been developed on child online threats.	• A set of globally accepted terminology is not available as yet.	• Clear understanding of online threats to children by all stakeholders and unambiguous application of laws for protection of children are required.

United Nations Children's Fund
India Country Office
UNICEF House, 73, Lodi Estate
New Delhi - 110003
Tel. : +91 11 24690401
www.unicef.in