INTERMEDIARY LIABILITY: CHILD PROTECTION

Dr. Gargi Chakrabarti*
Ms. Sonali Khatri & Ms. Aashna Jain**
National Law University, Jodhpur
India

ABSTRACT

Child protection in cyber space is becoming more complex with the increasing use of technology. India is no exception to the complicated nature of child protection in cyber space. Indian law is still being developed to ensure the protection of children online. However, these steps have proven insufficient thus far, as the number of cases of cyber bullying and child pornography is increasing at a phenomenal rate in India. Therefore, the role of online intermediaries has assumed significant importance in India. Such intermediaries are made liable for violation of child protection laws under certain conditions in India. This paper will analyze the statutory liability of intermediaries in India with respect to the issues of child protection. This analysis has been performed from the perspective of the Indian people, and has led to several recommendations regarding the future development of Indian laws on child protection.
I. INTRODUCTION

A child is a future asset in any country. But defining who is a child has remained a difficult issue in India for a long period of time. A variety of Indian pieces of legislation have adopted different age limits to define child and minors.¹ Therefore, the legal definition of the word child is ambiguous in India.² The Protection of Children Against Sexual Offences Act, 2012 overcame this challenge by defining child as any person who has not completed eighteen years of age.³ The United Nations Convention on the Rights of the Child (UNCRC), 1989 also defines child in a similar fashion.⁴ In 2011, India acceded to the UNCRC and ratified its Optional Protocol on the sale of children, child prostitution, and child pornography.⁵ For the purposes of the present paper, definition of child in India is will be a person below eighteen years of age.

India is the second largest country in world in terms of population, with 1.21 billion people.⁶ More than one-third of its population is below eighteen years of age, meaning there are approximately four-hundred million children in India.⁷ Around fifty percent of these children are in need of care and protection.⁸ The Indian legislative scheme intended to provide the framework necessary to develop a protective environment for all children focuses on providing care and protection to at-risk children and juveniles in conflict with law. These


³ Protection of Children Against Sexual Offenses Act, No. 32 of 2012, INDIA CODE, http://indiacode.nic.in, Section 2(d) (“child” means any person below the age of eighteen years”).

⁴ G.A. Res. 44/25, Convention on the Rights of the Child (Nov. 20, 1992), art. 1 (For the purposes of the present Convention, a child means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier).


Statutes and policies primarily aim to protect children from child labour, commercial exploitation, sexual abuse, and trafficking, as the targeted children are highly vulnerable in these areas.\(^9\)

An estimated 134 million Indian children will be active on the Internet by 2017, up from 39.5 million in 2012.\(^10\) It is important that children and their parents be aware of this sharp increase in use. This indicates how a substantial number of Indian children are using the internet at a tender and vulnerable age. Further, many children and their parents are not fully aware of the threats present online, and there is a rift between how children spend their time online and how parents perceive that their children spend time online.\(^11\) Children are becoming vulnerable to the risks of hacking, scam mails (like lottery wins),\(^12\) bullying, theft, and disclosing personal information to users who they do not know, including pictures, address, phone numbers, and e-mail IDs.\(^13\) The Indian legislature recognized the need to protect children in cyberspace due to the high risk of children being exposed to pornography and bullying in cyberspace.

**II. LEGISLATION IN INDIA REGARDING CHILD PROTECTION**

Various pieces of legislation, such as the Juvenile Justice (Care and Protection of Children) Act, 2000; the Protection of Children from Sexual Offences Act, 2012; and the Immoral Traffic (Prevention) Acts of 1956, 1986 and 2005, have been enacted to ensure child protection in India.\(^14\) A National Plan of Action for Children was developed, paralleling the enactment of the National Commission for the Protection of Children’s Rights Act, 2005.\(^15\)

---

\(^9\) United Nations Children’s Fund (UNICEF), *The State of the World’s Children 2011: Adolescence – An Age of Opportunity* (New York, 2011) (12% of India's children between the ages of 5 and 14 are illegally employed; around 50% are married before they turn 18; 50% face some form of sexual abuse, and a half of all girls between the ages of 10-13 are forced to drop out of school).


\(^12\) Id.


Also, the Integrated Child Protection Scheme was initiated in 2009.\textsuperscript{16} All these initiatives were created in order to ensure better protection of Indian children.

2.1 Information Technology Act, 2000

The primary source of cyber law in India is the Information Technology Act, 2000 (“IT Act”), which came into force on 17 October 2000.\textsuperscript{17} The Protection of Children Against Sexual Offences Act, 2012 also deals with child pornography.\textsuperscript{18}

Section 67B of the IT Act provides for the punishment of individuals for publishing or transmitting material depicting children in sexually explicit acts or conduct in electronic form.\textsuperscript{19} It also prohibits the creation of text or digital images and the collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or distributing of material in any electronic form that depicts children in an obscene, indecent or sexually explicit manner.\textsuperscript{20} Likewise, it is forbidden to cultivate, entice, or induce children to enter into an online relationship with one or more children for the purposes of a sexually explicit act or in a manner that may offend a reasonable adult on the computer resource.\textsuperscript{21}

\begin{itemize}
\item \textsuperscript{17} Dr. Savita Srivastava, \textit{Pessimistic Side of Information & Communication Technology: Cyber Bullying & Legislature Laws}, 1(1) INT’L J OF ADVANCES IN COMPUTER SCI. AND TECH. 14, 19 (Nov. – Dec. 2012).
\item \textsuperscript{18} Protection of Children Against Sexual Offenses Act, supra note 3.
\item \textsuperscript{19} The Information Technology Act, 2000, No. 21 of 2000, INDIA CODE, http://indiacode.nic.in, Section 67B (Whoever,-

\begin{itemize}
\item (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
\item (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
\item (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
\item (d) facilitates abusing children online or
\item (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

\begin{itemize}
\item Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
\item (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
\item (ii) which is kept or used for bona fide heritage or religious purposes

\textit{Explanation} - For the purposes of this section, "children" means a person who has not completed the age of 18 years).
\item \textsuperscript{20} \textit{Id.} at (b).
\item \textsuperscript{21} \textit{Id.} at (c).
\end{itemize}
\end{itemize}
bans the facilitation of the abuse of children online or records in any electronic form one’s own abuse or that of others pertaining to sexually explicit acts with children. The punishment for any of the preceding offenses upon a first conviction is imprisonment for a maximum of five years and a fine of up to ten lakh rupees. A second or subsequent conviction is punishable by imprisonment for up to seven years and a fine of up to ten lakh rupees. Section 66E of the Information Technology Amendment Act, 2008 [“ITAA, 2008”] criminalizes the intentional or knowing capture, publishing, or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, in circumstances where a person can have a reasonable expectation that:

(i) He or she could disrobe in privacy, without being concerned that an image of his private area is being captured; or

(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

This protection of privacy is very relevant in cases of child sexual abuse images that are increasingly being captured on mobile cameras.

---

22 Id. at (d), (e).
23 Id. at (e).
24 Id.
25 Information Technology (Amendment) Act, 2008, No. 10 of 2009, INDIA CODE, http://indiacode.nic.in, Section 66E (Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation — For the purposes of this section —
(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;
(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) “publishes” means reproduction in the printed or electronic form and making it available for public;
(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that —
   (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
   (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place).
2.2 The Protection of Children Against Sexual Offences Act, 2012

The Protection of Children Against Sexual Offences Act, 2012 prohibits the use of a child for pornographic purposes. The first conviction for use of a child for pornographic purposes is punishable by an imprisonment term of up to five years and fine, and in the event of a subsequent conviction is punishable by up to seven years of imprisonment and a fine. The Commissions for Protection of Child Rights Act, 2005 established the National Commission for Protection of Child Rights (NCPCR) in March 2007 as a statutory body. It was set up to protect, promote, and defend child rights in India. The Commission consists of a chairperson and six members who are well-versed in child welfare. The functions of the Commission, inter alia, include examining all of the factors that may impact the enjoyment of rights of children affected by terrorism, communal violence, riots, natural disaster,

Protection of Children Against Sexual Offences Act, supra note 3, at Section 13 (Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes – (a) representation of sexual organs of a child; (b) usage of a child engaged in real or simulated sexual acts (with or without penetration); (c) the indecent or obscene representation of a child; shall be guilty of the offence of using a child for pornographic purposes; Explanation – For the purposes of this section, the expression “use a child” shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of the pornographic material).

Id. at Section 14(1) (Whoever, uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also be liable to fine).


Id.

Id. at Section 3(1) (The Central Government shall, by notification, constitute a body to be known as the National Commission for Protection of Child Rights to exercise the powers conferred on, and to perform the functions assigned to it, under this Act.

(2) The Commission shall consist of the following Members namely : -

A Chairperson who is a person of eminence and has done outstanding work for promoting the welfare of children; and

Six Members, out of which at least two shall be women, from the following field, to be appointed by the Central Government from amongst persons of eminence, ability, integrity, standing and experience in,

(i) education;
(ii) child health, care, welfare or child development;
(iii) juvenile justice or care of neglected or marginalized children or children with disabilities;
(iv) elimination of child labour or children in distress;
(v) child psychology or sociology; and
(vi) laws relating to children.

(3) The office of the Commission shall be at Delhi).
domestic violence, HIV/AIDS, trafficking, maltreatment, torture and exploitation, pornography, and prostitution, and recommending appropriate remedial measures.31

2.3 State legislation: Goa

The State of Goa has pioneered the efforts to create a comprehensive law on child protection by enacting the Goa Children’s Act in 2003.32 It laid down child-friendly practices in tune with the UNCRC to be followed by the State of Goa and its courts. Under the section criminalizing “child abuse,” punishment is meted out for sexual assault, grave sexual assault, and incest.33 Soliciting children for purposes of commercial exploitation is prohibited, which includes hosting websites, taking suggestive or obscene photographs, and similar actions.34 The term “commercial sexual exploitation of children” is defined as “all forms of sexual exploitation of a child including visual depiction of a child engaged in explicit sexual conduct, real or stimulated, or the lewd exhibition of genitals intended for sexual gratification of the user, done with a commercial purpose, whether for money or kind.”35 The definition of “grave sexual assault” was expanded by the 2005 amendment, and now includes making children pose for pornographic photos and films, forcing minors to have sex with each other, and deliberately causing injury to the sexual organs of children.36 Developers of photographs or films, as well as Airport authorities, border police, railway police, and traffic police, have to report sexual or obscene depictions of children, suspected cases of trafficking of children, or other acts that violate the Act to the relevant authority.37

2.4 Discussions of Different Provisions

Children are the population most vulnerable to the dangerous effects of electronic media,38 yet there is no law that deals with cyber-bullying and online abuse specifically directed at children. Cyber bullying is a typical type of online harassment, which can include directing

31 Id. at Section 13(1)(d) (The Commission shall perform all or any of the following functions, namely :- (d) examine all the factors that inhibit the enjoyment of rights of children affected by terrorism, communal violence, riots, natural disaster, domestic violence, HIV/AIDS, trafficking, maltreatment, torture and exploitation, pornography and prostitution and recommend remedial measures).
33 Id. at Section 8.
34 Id. at Section 8(12).
35 Id. at Section 2(jj).
36 Id. at Section 2(y)(i)
37 Id. at Section 7(9).
38 Srivastava, Pessimistic Side of Information & Communication Technology, supra note 16.
harsh, rude, insulting, or teasing remarks through messaging platforms or in open forums, which may target one’s body shape and structure, educational qualifications, professional qualifications, family, gender orientation, personal habits, or outlook. It has been defined as “the intentional use of harmful words to put another person down.” When it was first enacted, the IT Act was completely silent on the issue of cyber bullying. It did not include any provisions relating to the prevention, punishment, or judicial procedure for crimes like cyber bullying. Cyber bullies could be covered under Section 67 of the IT Act, which punishes individuals for publishing information which is obscene in electronic form, and Section 72, which provides for penalty for breach of privacy and confidentiality. This helps to understand why the issues of cyber bullying, teasing, and hazing were not addressed properly under the IT Act, despite reports of suicides due to cyber bullying. Thereafter, certain amendments were proposed in 2007 and enacted in 2008. Under Section 66A of the IT Amendment Act, 2008, cyber bullying was addressed, and was punishable with three years of imprisonment and a fine. Subsequent cases of cyber bullying were dealt with under


40 Id.


42 ITAA, 2008, supra note 26, at Section 67 (Punishment for publishing or transmitting obscene material in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees).

43 Id. at Section 72 (Penalty for breach of confidentiality and privacy.—Save as otherwise pro- vided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both).


this Section, although there is no explicit use of the word “cyber bullying.”48 The Section provided for the punishment of offenders with imprisonment and a fine for sending offensive messages through a communication service or similar acts.49 The phrase “offensive messages” was interpreted to mean cyber bullying.50 The word bullying should not be given any technical or water-tight meaning. It should instead be understood in common parlance. However, these amendments to the IT Act were not felt to be adequate enough to cover the issue of cyber bullying in a comprehensive manner in India. A separate provision on cyber bullying is felt to be required in order to adequately protect children.51 Currently, there is no provision in India dealing specifically with cyber bullying due to the Supreme Court of India’s striking down of Section 66A, holding that the criminalization of speech is acceptable only in very narrow set of circumstances.52 This removed the only provision of the IT Amendment Act directly addressing cyber bullying, and has left a statutory void in this regard.

III. LEGAL ANALYSIS OF THE INTERMEDIARY LIABILITY LAWS IN INDIA

The provisions of the IT Act and Information Technology (Intermediary Guidelines) Rules, 201153 (“IT Rules”) have imposed certain guidelines on the activities of Internet Service Providers (“ISPs” or “intermediaries”). The definition of an “intermediary” has been provided under Section 2(w)(1) of the IT Act54. Under the IT Act, “intermediary” means “any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.”55 Section 79 of the IT Act provides exemptions from liability of ISPs in certain cases.56 This section grants immunity to ISPs when they act

---

48 ITAA, 2008, supra note 26, at Section 66A.
49 Id.
52 Shreya Singhal v. Union of India (2012), Writ Petition (Criminal) No. 167 of 2012 (India); Shweta, Cyber Bullying, supra note 40.
53 Information Technology (Intermediary Guidelines) Rules, 2011, Gazette of India, pt. III sec. 4 (Apr. 11, 2011) (notified in April 2011, these rules were enacted by virtue of section 87(2)zg and section 79 of the Information Technology Act, 2000).
54 IT Act, supra note 19, at Section 2(w)(1).
55 Id.
56 Id. at Section 79 (INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES:
as mere conduits and do not initiate the transmission, select the receiver, or select or modify the information contained in the transmission. An ISP will not be liable if the offence or contravention was committed without its knowledge, or it exercised due diligence to prevent the commission of the offence or contravention.  

3.1 Due Diligence Under the IT Rules, 2011

The IT Rules also set forth how intermediaries exercise due diligence. This Rule lays down the regulations to be followed by the intermediaries when exercising due diligence for the purpose of exemption from liability.

A. Due Diligence of the Intermediaries

Rule 3 of the IT Rules lays down the duties of the intermediaries. This does not point out the fact that there is no corresponding liability of censorship or for the moment when the objectionable content is made available online. The relevant provision states that it is the duty of the intermediary to publish all the necessary policy statements, rules, and regulations. Also, it is the duty of the intermediary to observe activity conducted through it and notify the users that the information published should not be pedophilic, pornographic, or harm minors.

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

(2) The provisions of sub-section (1) shall apply if—
   (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or
   (b) the intermediary does not—
      (i) initiate the transmission,
      (ii) select the receiver of the transmission, and
      (iii) select or modify the information contained in the transmission;
   (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—
   (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorize in the commission of the unlawful act;
   (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

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

57 Id.
58 Id.
60 Id.
Some of the important requirements of the due diligence element are discussed herewith.

**B. Rationale Behind Intermediary Liability**

The intermediary shall not itself host, publish, edit, or store any information, and shall not initiate the transmission, select the receiver of transmission, or select or modify the information contained in the transmission, which is mentioned in sub-Rule 3. Therefore, a logical conclusion is that intermediaries are not liable simply because they provide the platform through which material is published, whereas the user who actually uses that platform for their activities bears primary responsibility.

**C. Complaint Mechanism**

When an intermediary has actual knowledge that a person is affected by any post, then cognizance will be taken in 36 hours and that post will be removed or disabled within those 36 hours. The rule uses ambiguous and vague terms like “actual knowledge” and “affected

---

61 Id. at Rule 3(2) (The intermediary shall notify users of computer resource not to use, display, upload, modify, publish, transmit, update, share or store any information that:—

(a) belongs to another person;
(b) is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, pedophilic, libelous, invasive of another’s privacy, hateful, or racially, ethnically or otherwise objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
(c) harm minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) discloses sensitive personal information of other person or to which the user does not have any right to;
(g) causes annoyance or inconvenience or deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
(h) impersonate another person;
(i) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
(j) threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

62 Id. at Rule 3(3) (the intermediary shall not itself host or publish or edit or store any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2)).

63 Id. at Rule 3(4) (the intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes).
person” without defining them. The question arises as to who counts as an “affected person,” and what is his locus standi of complaining to the intermediary. Also, the phrase “actual knowledge” brings the dispute as to what set of facts signifies that the intermediary had “actual knowledge” of the said dispute or grievance.

D. Disclosure of Information to the Government

Intermediaries are obligated to provide information, upon demand, to the Indian government agency that enforces cyber security or any other investigation team in order to help discover the identity of the author of the disputed content.

E. Reasonable Measures

The intermediary is supposed to take all reasonable measures to secure its computer resources and information contained therein. Therefore, it is required to follow reasonable security procedures and practices. The requirements for such reasonable measures have been provided by Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

F. Grievance Officer

According to Sub-Rule 11 of Rule 3, the officer named on the intermediary’s website is bound to receive complaints and must respond to them within a month.

---

64 Id. at Rule 3(3)(b).
65 Id. at Rule 3(7) (when required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorized for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.
66 Id. at Rule 3(8) (the intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011).
67 Id. at Rule 3(8).
68 Id. at Rule 3(8).
69 Id. at Rule 3(11).
3.2 Discrepancy with the Constitution of India

Compatibility with Article 19(1)(a) and (2)

Article 19(1)(a) of the Constitution of India guarantees freedom of expression, although this freedom is subject to reasonable restrictions provided under Article 19(2) of the Constitution. In cases where a person, while exercising the freedom provided under Article 19(1)(a), exceeds it in such a way that the expressed speech is detrimental to child protection, then it will be actually be a violation of the freedom of speech and expression. But when a case does not clearly fall within these protections or is subjective, freedom of speech and expression rights in relation to child protection will become a debatable matter. In Romesh Thappar v. State of Madras, the Supreme Court held that the freedom of speech and expression under Article 19(1)(a) includes the freedom to propagate and disseminate ideas. It also held that there are narrow circumstances under which there may be a legislative ban on the right to free speech. Also, the Supreme Court held in Express Newspapers (Private) Ltd. v. Union of India that any restriction on 19(1)(a) which falls outside Article 19(2) is invalid.

Also, free speech should be respected across all mediums of communications, such as the Internet, television, radio, and newspapers. There should not be any arbitrary distinction between such mediums. In Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal, the Supreme Court’s decision reflected the understanding that where media platforms are sufficiently different, such that their treatment must be different in accordance with those indicia of difference, it will treat them as such in order to uphold

---

70 INDIA CONST. art. 19; IT Rule 3(2), supra note 61.
71 INDIA CONST. art. 19 (Protection of certain rights regarding freedom of speech etc.

(1) All citizens shall have the right
   (a) to freedom of speech and expression;
   (b) to assemble peaceably and without arms;
   (c) to form associations or unions;
   (d) to move freely throughout the territory of India;
   (e) to reside and settle in any part of the territory of India; and
   (f) omitted
   (g) to practice any profession, or to carry on any occupation, trade or business

(2) Nothing in sub clause (a) of clause ( 1 ) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence).

73 Id.
74 Express Newspapers (Private) Ltd. v. Union of India, AIR 1958 SC 578 (India).
fundamental rights. Finally, in *Ajay Goswami v. Union of India*, the Supreme Court stated that the Internet, being a novel innovation, deserves a unique and different benchmark of protection when compared to its ancestors. It can be concluded from these cases that complexity and vastness of cyberspace is much greater than the physical world.

Rule 3(2) of the Intermediary Guidelines, which lists the grounds for censorship, is not compliant with Article 19 (2) for two reasons. Firstly, many grounds, such as grossly harmful, hateful, or disparaging, do not have any constitutional basis. These terms do not have any objective criterion to be determined and are hence very arbitrary and subjective. Secondly, these restrictions are unreasonable because the Rule is not properly addressing the “disparaging speech;” hence, the penal provisions are not specific according to the regulation.

**Compatibility with Article 21**

In *People’s Union for Civil Liberties v. Union of India*, the Supreme Court held that Article 21’s privacy rights protected individuals against the interception and monitoring of private communications by the government in the absence of sufficient safeguards.

According to the IT Rules, cyber cafés are included within the ambit of intermediaries. This inclusion is relevant to child protection laws in two respects: (i) according to the Indian socio-economy, most of the Indian can avail computers in cyber cafés only, and (ii) they cannot afford a personal computer for their own use. But computers can be used for the enhancement of education and enriching the knowledge of school children. In order to use a computer in a cyber café, children need to show their identity card or else he or she needs to be accompanied by an adult. In India, children usually do not have identity cards (except school identity cards from very selective private schools of urban India, and Aadhar cards for some children in recent years) for themselves; this requirement may hinder children’s access

---


77 People’s Union for Civil Liberties v. Union of India, AIR 1997 SC 568 (India).

78 Section 2(1)(w), Information Technology Act, 2000: “intermediary”, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafés.

79 IT Rules, *supra* note 53, at Rule 4(3) (children without photo identity card shall be accompanied by an adult with any of the documents as prescribed in sub-rule (1)).
to the Internet if they are unaccompanied by an adult. Moreover, a log book maintained by the cyber café may represent a threat to children, because the content of the log book is not specified in the Rule and it is left within the discretion of the cyber café.\textsuperscript{80} Hence, there is no guarantee that the log book would not be misused or mishandled by the occupier or any other person, and it can be a potential threat to both personal data privacy and child protection.

IV. POLICIES OF INTERMEDIARIES

The three most popular communicating intermediaries over the internet are Facebook, YouTube, and Twitter. There is a need to analyze whether these intermediaries are strictly following the obligations and liabilities of the IT Rules of India.

\textbf{FACEBOOK}\textsuperscript{81}

Facebook does not guarantee to remove any content that is reported to be in violation of India’s laws. Facebook’s content viewers will reach out to the people who object to the content, and then they will make a decision to remove the content if it is in contravention of Facebook’s Community Standards. Facebook guarantees to instantly remove content depicting any form of child exploitation. Facebook has a specific “Community Standard” policy for “Sexual Violence and Exploitation,” and this includes the sexual exploitation of minors. The Facebook definition of “Sexual Exploitation” includes solicitation of sexual material, any sexual content involving minors, and threats to share intimate images and offers of sexual services; it can be said that for the protection of victims, Facebook’s policy guarantees the removal of photographs and videos depicting incidents of sexual violence. But it is within the sole discretion of Facebook to judge whether the content in a particular post violates their “Community Standards.” The removal is based solely on abuse reports submitted by viewers, because Facebook’s own screening process is not clarified under its policy.

\textbf{YOUTUBE}\textsuperscript{82}

YouTube has a specific policy that if the content is sexually provocative, it is less likely to be


\textsuperscript{81} Terms and Policies, FACEBOOK, \textit{available at} https://www.facebook.com/policies/?ref=pf (last visited June 29, 2015).

\textsuperscript{82} Terms of Service, YOUTUBE, \textit{available at} https://www.youtube.com/t/terms (last visited Aug. 27, 2015).
acceptable. Also, content like child pornography, nudity, or other sexually explicit content may not be uploaded. A video that contains nudity or other sexual content may be allowed if the primary purpose is educational, documentary, scientific, or artistic, and it is not gratuitously graphic. For example, a documentary on breast cancer would be appropriate, but posting clips out of context from the same documentary might not be. YouTube provides a mechanism for flagging the video in order to report the content. YouTube also suspends the accounts of users who try to upload any material which involves the endangering of children. The flagged videos are reviewed every 24 hours by YouTube, and are taken down if found inappropriate. YouTube also claims to suspend the accounts of repeat infringers.

**Twitter**

Twitter does not take any responsibility for material that is posted by users on its website, and does not even promise to monitor or control the content being posted. Twitter also does not guarantee the completeness or truthfulness of the data. However, it reserves the right to suspend the accounts of users. Twitter has a system of flagging objectionable material or sensitive content, but does not guarantee the removal of the same. The flagged content will not even receive an automatic warning message from Twitter. However, Twitter does not tolerate child exploitation.

*Analysis of the Policies of these three intermediaries:*

- It can be deduced from the terms and conditions of Facebook that they are in partial compliance with the IT Rules as far as publication policy and child exploitations are concerned.
- YouTube’s policies are very straightforward and strict. They have no tolerance for child exploitation, and they have a complete mechanism of flagging, reviewing, and removing content if it is found to be offensive. Therefore, it can be very clearly said that YouTube is almost fully compliant with the IT Rules.
- Twitter has very practical policies of flagging the content as sensitive or offensive, which ensure that there is no area of dispute that may expose certain people to content which is unsuitable for their age or is otherwise inappropriate. Also, Twitter has a perfect review mechanism. It does not take responsibility of the content that is put up on the website. In addition, it does not tolerate child exploitation. Hence, it is in

---

The definition of “intermediaries” has been provided under the IT Act. Under this definition, Airtel and MTNL, which help users connect to the Internet by means of wired or wireless connections, are intermediaries.\textsuperscript{84} Therefore, it is imperative to look at their policies to examine if they are complying with the rules and regulations governing intermediaries in India, along with other entities:

**Bharat Sanchar Nigam Limited (BSNL)** states that the subscriber is required to comply with the provisions of the IT Act.

**Vodafone** does not accept responsibility for any use of their service by their clients. It does not restrict the posting of obscene, offensive, and annoying information.

**Airtel** directs its customers to not resort to any offences of hacking, cracking, and spamming, and reserves the discretion to discontinue its services if the user commits any of the offences defined in the IT Act. Also, it reserves the right to access customers’ information in case there is a breach of the aforementioned laws.

**Tata DoCoMo** prohibits its users from posting or transmitting some categories of material, and also undertakes to conduct periodic reviews to prevent the uploading of offensive material. However, it disclaims any liability for failing to do so whether under contract, statute, or the law of equity or of torts.

After analyzing the policies of all the leading Internet connection providers, it can be concluded that, when any customer is utilizing their connection and dealing with obscene, offensive, or sexually explicit material, the connection provider is not responsible until any complaints are received or any legal proceedings are initiated against them.

Despite these policies, the actual use of these services in India is not very satisfactory. The Internet is constantly used for the transmission and distribution of offensive material, which raises the issues of child protection.

\textsuperscript{84} IT Act, *supra* note 19, at Section 2(w) (“Intermediary”, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes).
There are also instances when court orders produce debatable or conflicting situations regarding cyber-related crimes. According to a Madras High Court order, Airtel and Reliance Communications had to block Vimeo and DailyMotion.com in May 2012 due to their illegal hosting of copyrighted material. But in reality, the same material was available from the infringing sites through other ISPs, like Tata DoCoMo. If hosting certain copyrighted material on the Internet amounts to infringement, it has to be considered a violation of law in all analogous cases, so similar orders should be given for all the ISPs instead of only a select few. So, the Court order should apply to all the ISPs operating at that point of time in the said jurisdiction (in this case, throughout India).

V. PRACTICAL INSTANCES OF VIOLATION OF CHILD PROTECTION

No one can deny that Internet-related laws and rules are in the development stage in India. In response to the technological advancement and the demands of the situation, amendments are being made in the law. So, the growth and strengthening of the legal regime have been seen over time. Still, the constraints in formulating a legal solution in relation to cybercrime are two-fold: firstly, the understanding of physical crime is much clearer so authorities attempt to figure out cybercrimes in the same manners as physical crime; and secondly, the availability of infrastructure and know-how is limited amongst the police personnel and other officers of law and order. Very few people are trained to deal with cybercrime and dedicated Cyber Cells are available in very few cities in India, so most of the complaints of cybercrime are dealt with just like physical crime by most of the officers of law and order. Now India is going through the transitional period; now it is the time to realize that it needs proper training to handle cybercrime, which will give the insight to take a different approach to handling physical crime and cybercrime. To date, the number of cyber law cases is very few in India, so the scope of interpretation of legal statutes by analyzing the decided case is limited. A countrywide empirical study needs to be done regarding the types of complaints lodged in police stations (First Instance Report or FIR) for cybercrime, and the kind of responses generated thereafter. Instances of cybercrime are sometimes reported in newspapers; usually not elaborately but in a very brief manner. So the researchers of this paper have gathered several brief instances of cybercrime related to child protection from various newspaper reports:

• A young girl at one of the top colleges became depressed when an old picture of her, from one of her social media accounts, went viral and became the centre of criticism of many students.86

• A boy committed suicide because of a video posted by his friend on the internet. In that video, he was found in a compromising situation with his cousin.87

• One boy outshone his school seniors in basketball. Out of jealousy, his seniors harassed him online. Consequently, the boy stopped playing basketball anymore. He withdrew himself from his school activities.88

• Ms. Aparna (name changed) spurned her friend who, angered by the rejection, circulated a nude picture of her on the web. The boy morphed her picture, checked into her email account, and sent it to all the people in the contact list.

• Sujatha (name changed) decided to close her social media accounts and discussed this with a few friends too. A few days later, both her Facebook and Gmail accounts were found in a compromised situation. Obscene pictures were also posted on them.

• A teenager in Chennai, India was arrested for publishing child pornography by creating a Facebook page and by posting the images of female children. Some sexually explicit comments were also posted along with the images. A case was registered, and the profile was removed and the person was remanded to judicial custody.89

• The cyber wing of CB-CID in Chennai arrested an employee (who was married and had children) for mistakenly sharing a child porn picture in an office WhatsApp Group. He was arrested under sections 67, 67-A, 67-B of the Information Technology Act and Section 14 of Protection of Children from Sexual Offences (POCSO) Act.90

86 Alawadhi, supra note 48.
VI. Empirical Data

Due to the increased instances of bullying and pornography over the Internet, a survey was conducted among a group of forty people to discover their view towards the role of intermediary liability in child protection. The surveyed adults were from diverse groups. A mixed set of responses was received from them on the questions, which are represented below in the form of pie charts.

1. Do you think that unregulated Internet use is safe for children?

[Image of pie chart showing 100% "No"]
2. Do you think that parents should keep watch on their children’s online activities?

![Pie chart showing whether parents should keep a watch on the online activities of children](image)

3. What threats/dangers is a child likely to face on the Internet?

![Pie chart showing threats/dangers a child is likely to face on the internet](image)
4. Do you think that children can be bullied online?

[Pie chart showing percentages: Yes 82%, Yes with greater ease 12%, No 6%, May or May not 0%]

5. How can a child’s Internet activities affect his behavior and mood?

[Pie chart showing percentages: Inappropriate Behavior 45%, Become Psychologically Weak 22%, Lack of ability to handle cyber world 11%, Distance with Parents 11%, Affects Comprehending Skills 11%]
6. Should websites such as Facebook, Twitter, etc. allow children below 14 years of age to use their website?

**Should websites such as Facebook, Twitter, etc. allow children below 14 years to use the website?**

- Yes: 23%
- No: 62%
- 16 years is appropriate age: 15%

7. Do you believe that social media websites make the commission of crimes such as kidnapping and stalking easier?

**Do you believe that social media websites make the commission of crimes such as kidnapping and stalking easier?**

- Yes: 85%
- No: 15%
8. If I can obtain links to websites sharing child pornography on Google, should Google bear any responsibility for the same?

9. What steps should be taken to ensure child safety on the Internet?
6.1 Analysis of the data

A significant number of people think that there should be monitoring by the parents of their children’s activities online. The remaining people do not support non-monitoring per se, but think that monitoring is not practically possible. This points to their lack of awareness on the subject of online child safety. In the recommendations section below, the researchers have tried to highlight how online child safety can be promoted, and thereby address this problem of lack of awareness.

A significant number of people are aware that children are exposed to a variety of threats online. The survey also shows that the parents do not specifically know the extent of such threats. They still adhere to the traditional notion of disclosure of personal information online being the sole or primary threat of the Internet, and are still unaware about the threats of cyber bullying and child pornography.

Surprisingly, there was a unanimous response that access to social networking sites such as Twitter and Facebook should not be provided to children below fourteen years of age. This reflects an acknowledgment that lower-age users of these sites are at greater risk of bullying.

A large proportion of the surveyed population believes that intermediary liability should be more stringent in the case of heinous offences, such as child-pornography. It points to the need of a complete overhaul of the policies of the intermediaries themselves, such as YouTube, many of which are owned by Google. This response is contrary to the current practice of the Indian people, who have not taken the initiative in requesting Google to remove content from its products. From January 2014 to June 2014, a total of 250 cases were reported in which people requested Google to remove certain objectionable content.91 Out of these cases, only 48 requests were made on account of adult content, cyber bullying, and nudity. The majority of requests for content removal came for Gmail (114) and the least for Blogger (46). There has been a very minimal compliance by Google with court orders (11%) and law enforcement agency requests (8%).92 Lastly, the survey shows that cooperation between all sections of Indian society is required for meaningful online child protection, which could be in the form of supervision by parents, increasing the age for accessing the social networking sites, or other measures.

92 Id.
VII. RECOMMENDATIONS AND CONCLUSION

Parents need to realize that granting their children unlimited freedom when using the Internet may lead to their children browsing content which is unfit for their tender age, or may expose them to cyber bullying, cyber phishing, or other harmful activities on the Internet.

_Sample Survey by McAfee (2011)_

- While 54% parents have generic security software on their PCs, a massive 77% are unaware of the specific software available to monitor child safety online.93

- In Delhi, 50% parents allow their kids to spend more than 10 hours a day on the Internet.

- 25% of parents trust their children online without monitoring them. But the level of the trust increases with the increase in the age.

- Only 2% parents had heard about the emerging online threats, such as cyber stalking and cyber bullying.94

- Of all Indian cities, parents in the cities of Bangalore and Ludhiana had the least awareness of online activities of their kids.

These findings are vital for the children as well as their parents. They indicate how Indian children are being affected online at a tender age. They also reveal that Indian children are spending more time socializing on the Internet with friends than in real life, especially in the nine to twelve years-old category. Further, many children and their parents are not fully aware of the threats present online, and moreover there is a rift between how children spend their time online and how parents perceive how their children spend time online.95 Children are becoming vulnerable to the risks of hacking, scam mails (like lottery wins),96 stalking, bullying, theft, and disclosing personal information, including pictures, address, phone numbers and e-mail IDs, to others.97 Data also points to the inadequate monitoring of online

---

93 Intel Security, Inc., _Excerpts_, supra note 11.
95 Intel Security, Inc., _Excerpts_, supra note 11.
96 Id. (experience of Abhishek Goenka, one of the Panelists at the Panel discussion).
97 Indo Asian New Service, _Indian Parents_, supra note 13.
activities by the parents.\textsuperscript{98} Based on the findings of this paper, several suggestions are given by the researchers so as to enhance the online safety of the children, which are described below.

### 7.1 Traditional Methods

Parents can simply limit their child’s time spent online. Also, they should decide which sites may be accessed. The sites related to adult content, gambling, or other potentially harmful activities can be blocked. Parents can also participate in a basic course in ethical hacking so that a clever child does not easily break the blocks created by parents.

There are many advanced products, such as AVG Family, which should be used if the child is blocked from the access of specific websites. Among many other advanced features, these products can limit access to games based on Entertainment Software Rating Board (ESRB) ratings, monitor instant messaging conversations, and even push control up into the home router so that all devices, PC and otherwise, are covered.\textsuperscript{99}

### 7.2 Hardware-Based Control

Parents can also use a more advanced form of monitoring, such as a scheduled form of checks. In this system, the hardware helps with web content filtering and also in the Internet time scheduling. Here, the best aspect is that it has utility across all the devices that are connected to the Internet, including iPods, Personal Computers, or Tablet PCs. This method does not provide the detailed information and monitoring as may be available with software-based control methods. Instead, this is a generalized method of monitoring and hence it can, in very rare cases, be configured per individual requirements.

### 7.3 Mobile Applications

Recently, parental control applications on mobile phones and computers are becoming increasingly common. The parents can keep track of which sites the child is visiting. Also, they get warning messages if the child leaves the designated online safety zones. There are certain parent facilitation apps which allow the parents to track the continuous movement of their child online, such as the E Blaster Mobile app for Android. There are also certain

\textsuperscript{98} Intel Security, Inc., \textit{Excerpts}, supra note 11.

companies that provide applications that lock down the devices if the child goes against the standards set by the parents.  

7.4 Social Network Safety

There are certain apps that allow parents to know what their child is posting to social media and to what posts to which their child is being exposed. Additionally, these apps have the capacity to highlight posts and messages that might indicate cyber bullying. There are also certain unique apps that allow the parents to monitor what information is made public, and hence aim at making privacy settings stronger.

7.5 Simple Spyware

There are certain advanced apps that allow parents to spy on their children, in the proper sense of the word. These apps are used in a stealthy way, and take certain automatic screen shots, can retain the log-keyboard strokes, and otherwise closely monitor children’s Internet activity. These advanced apps are necessary only in certain high-level problems, such as where there is a possibility that the child is communicating to a pedophile and where the conversations with that person must be retained.

There is an urgent need for a complete overhaul of the current system of online child protection. The statistics suggest that the parents are not aware of the potential threats that their children are exposed to daily. In a country like India, child protection is urgently needed in the urban and sub-urban areas because of the fact that Internet connectivity is greater in the cities than in rural areas; the use of certain safety software and devices can be a remedy for the potential threat.

7.6 General Guidance

Computer education is not compulsory in all schools in India and computer literacy levels are not up to the mark in children as well as their parents in many parts of India; the consequent lack of awareness is a genuine problem. Children’s use of the Internet implicates not only the problems of child pornography and cyber bullying, as children may also face undue influence from cyberspace that may be misleading and may result in kidnapping or child trafficking. That is why continuous vigilance at school (by the teachers) and at home (by the parents) is

---

100 Example: Norton.
101 Example: Safety Web.
102 Examples: Spector Pro, PC Pandora.
necessary for the protection of children online. For that, teachers and parents need to have the capacity to deal with the consequences of advances in technology. Not only that, but child behavior must be constantly monitored by the teachers and parents very meticulously, which can lead to early diagnosis of any problem faced by the children from online activity. Cooperative approaches in supervision by parents of any particular child, parents of other children, and teachers would be helpful, and any such change in child’s behaviour should never be ignored, but rather should be reported, investigated, and taken care of.