OUR ESTEEMED PARTNERS

Bureau of Police Research and Development
Ministry of Home Affairs
पुलिस अनुसंधान एवं विकास ब्यूरो, गृह मंत्रालय

NCPCR

HANDBOOK ON CYBER CRIMES AGAINST CHILDREN AND INVESTIGATION METHODOLOGIES FOR LAW ENFORCEMENT AGENCIES

CYBER PEACE FOUNDATION

unicef
for every child

CYBER PEACE FOUNDATION

unicef for every child

TABLE OF CONTENTS

CYBER PEACE FOUNDATION

unicef for every child

TABLE OF CONTENTS

About the Handbook

This handbook is designed to act as a ready reference for Law Enforcement Officials and prosecutors to understand cyber crimes against children. Cyber Crimes are generally defined as those crimes in which a computer resource is either the target or is used as a tool for committing the crime. These may even include cases where traditional crimes are facilitated by digital technologies as will become clear through the course of this handbook.

This handbook focuses on presenting a clear picture of cyber crimes committed against children and when cyber crimes have been perpetrated by them. It also helps Investigating Officers to understand the application of special legislations like the Information Technology Act, Protection of Children from Sexual Offences (POCSO) Act and Juvenile Justice (Care and Protection) Act to such instances.

This handbook is a result of secondary research, interviews with law enforcement officials, lawyers and practitioners of the domain. The need for this handbook was felt during ToT (Training of Trainers) workshops with law enforcement officers. Then, post the ToT it was through a series of consultations and a few pilot workshops that UNICEF and Cyber Peace Foundation came together to identify specific gaps in the entire chain of investigation and prosecution of cyber crimes against children, starting from the first response and leading all the way to conviction of an offender.

CYBER PEACE FOUNDATION

unicef
for every child

PART - I
Understanding Cyber Crimes Against Children

Why is there a need for sensitization about Child Specific Cyber Crimes?

While interacting with children, there are some specific things which need to be factored in by an Investigating officer and that also form the basis for sensitization about child specific matters.

They are easily trusting

It is easy for perpetrators to win over a child's trust and then lure him into illicit activities. Children, in their innocence tend to easily believe strangers.

They don't react like adults

When spoken to rudely, they will be scared. When shown pity, they will become cautious and when forced to speak, they might not speak at all. They may even be hesitant and ashamed to talk about an incident sometimes.

They don't understand abuse and criminal activity

Owing to lack of understanding and innocence, a child may be continuously abused and harassed and still be unaware about it. This poses the challenge of getting relevant information for an investigation by the Investigating Officer.

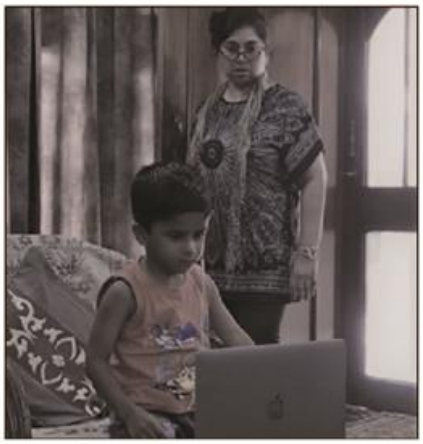
There are special laws and procedures

Often, the modus operandi of an offender in case of a conventional cyber crime could be so ill-fitting for a cyber crime against a child that it might lead to the assumption that an offence has not been committed. To address this need, special laws like the Juvenile Justice Act and the POCSO Act have been enacted. Not just that, special provisions in existing legislations like the IPC and IT Act have also been added to deal with sensitive matters involving children.

Threats to Children in the Digital Age

1. Online Sexual Abuse of Children

Sexual Abuse of children is forcing, luring or persuading a child by a person, male or female, to take part in sexual activities, which may happen with or without physical contact, offline or online. Such abuse may even be committed without explicit force. The mere fact of some sexual activity taking place is sufficient to constitute abuse. Sexual activity may include touching or exposing private body parts of a child or even showing him something sexually explicit. Child sexual abuse can take the form of both contact and non-contact abuse. Contact abuse refers to forced physical abuse of a child which includes acts ranging from touching with a sexual intention to penetrative assault. Non-contact abuse which includes online child sexual abuse could be passive as in the case of exposing children to inappropriate



online/offline content or an active sexual solicitation like using threats, force or lures to extort their nude pictures/videos to force them into sexual conversations. When it happens online, there might not even be any type of interaction between the offender and the victim at all which increases the challenges for an Investigating Officer on such crimes.

*Understanding Sexual Assault under the POCSO Act**

Activity	*Imprisonment*
Penetrative Sexual Assault (Sec 3) *Inserting body part or object in a child, or making a child do this with another*	Not less than seven years of imprisonment, may extend to life (Sec 4)
Aggravated Penetrative Sexual Assault (Sec 5) • *Penetrative sexual assault by a police officer or person responsible for care.* • *Using deadly weapons or substances* • *Causing physical/mental illness or incapacitation,* • *Making girl child pregnant,* • *Attempting to murder or causing grievous hurt* • *Or on a child younger than 12*	Not less than ten years of imprisonment, may extend to life (Sec 6)
Sexual Assault (Sec 7) *With sexual intent touching the private parts of a child*	Not less than three years of imprisonment, which may extend to five years (Sec 8)
Aggravated Sexual Assault (Sec 9) *Non penetrative sexual assault by a police officer, member of armed forces, public servant, staff of remand home/jail/hospital/school, etc, and other acts of sexual assault by any person as mentioned in the second part of section 5, except making a girl child pregnant*	Not less than five years of imprisonment which may extend to seven years (Sec 10)

**These are not exhaustive provisions, a reader may refer to the POCSO Act for the exact language*

Non-contact online abuse is addressed under Section 11 of the POCSO Act. Broadly referred to as sexual harassment, verbal acts, showing pornography to a child, threatening to use depiction of a child involved in a sexual act, and enticing a child for pornographic purposes constitute non-contact abuse and are criminal offences.

Exposure to sexually explicit content

i. Sending/Sharing/Exposing a child to pornographic or other sexually explicit content in any form

ii. Criminalized under Section 11(iii) of the POCSO Act – up to 3 years imprisonment

iii. Even when the offender exhibits his own body parts (Section 11(i))

iv. if someone exposes a child to words, gestures or sounds made with a sexual intent, such person shall be liable for a punishment of imprisonment for a term of three years under Section 11 (i) of the POCSO Act . Section 67A of the IT Act may also be used when direct messaging, publishing of any such material – up to 5 years; even includes graphic comics, animations made with the intention of being pornographic

v. Section 67 may be used when obscene content sent (not necessarily sexual) but lascivious (depicting sexual interest, trying to excite sexual desire)- up to 3 years imprisonment

Enticing a child for sexual favors

i. Luring, attracting, tempting a child with sexual intent

ii. Through offering game rewards, money etc.

iii. Criminalized by Section 11(vi) POCSO Act – up to 3 years imprisonment

iv. But offence under the POCSO Act is bailable

v. Under Section 67B(b) - cultivating, enticing or inducing a child into online relationships for sexually explicit acts and conduct, punishment – up to 5 years, non bailable

Making a child exhibit his body parts

i. Forcing or enticing a child to show his body parts to the offender or to anyone else

ii. Criminalized under Section 11(ii) of the POCSO Act – up to 3 years imprisonment

iii. No specification of medium: may be through video sharing, live streaming, video calling etc.

Facilitating abuse of children

i. Facilitation of abuse could be through operating websites, portals, forums, chat groups specifically for proliferation of sexually explicit content involving children or to aid any other abuse of children

ii. Section 67B(b) of the IT Act applies- up to five years

iii.Sections 16 and 17 of the POCSO Act may also apply for abetting any activity under POCSO Act

Online Trafficking of Children

Although not exactly an offence under the POCSO or IT Act, Online Trafficking is an activity that is a gruesome manifestation of the offline crime of the similar nature. NCPCR's Child Victims of Cyber Crime Legal Tool Kit identifies how IPC provisions apply to cases where children are lured and then trafficked using online modes as well. It identifies Section 5 of the Immoral Traffic Prevention Act, 1956 that prescribes punishment of rigorous imprisonment for not less than three and not more than seven years for persons who either procure, induce or take a person for the sake of prostitution. In cases where a minor girl is procured, Section 366A of the IPC applies as well if she is induced or forced and there is a likely threat that she will be seduced into illicit intercourse. Such activity of procuring or inducing is punishable with up to ten years of imprisonment.

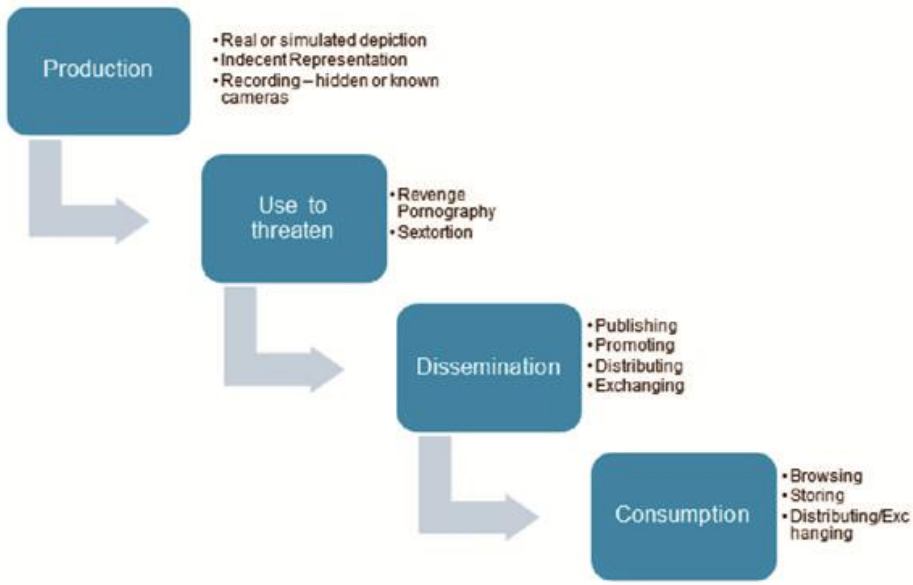
Source: NCPCR's Child Victims of Cyber Crime Legal Tool Kit

2. Online Sexual Exploitation

Children in exploitative situations and relationships are offered or receive something such as gifts, money or just attention and affection as a result of performing sexual activities or others performing sexual activities on them. Child sexual exploitation doesn't always involve physical contact and can happen online. When sexual exploitation happens online, young people may be persuaded, or forced, to:

- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone
- have sexual conversations by text or online

It is generally done to use them for sexual gratification, creating pornographic content, extortion for money/continued favors etc. The biggest vertical of online sexual exploitation against children is the increased demand and consumption of Child Sexual Abuse Material (CSAM).



Child Sexual Abuse Material (CSAM) or what is more commonly known as child pornography is material depicting acts of sexual abuse and/or focusing on the genitalia of the child. Such material need not be in the audio/video format only and also cover indecent representations of children through animations, comic strips, graphics etc.

Production of CSAM (Child Sexual Abuse Material)

i. Using a child for pornographic purpose (real or not), any indecent representation of a child- criminalized under Sections 13 and 14 of POCSO – up to 5 years of imprisonment

ii. Creating text or digital images (including videos) punishable under the IT Act also: Section 67B(b)- 5 years of imprisonment

iii. When one directly participates in the sexual acts being shown in the content , in addition to the punishment under Section 13 and 14 of the POCSO Act - also liable for sexual assault as highlighted

Case Study: Sheena (Name Changed)

Sheena was a 16 year old school girl who liked a Pakistani singer very dearly. One day she received a friend request from a profile that had the singer's picture as the display picture and the same name as his. She accepted the request and somehow she was made to believe even that it was him.

After months of chatting online and speaking on the phone, she shared some intimate pictures of hers with the imposter. He then spoke to Sheena on the phone once and it was clear to her that it was actually someone else. Scared, she went to her mother who was the sole bread earner and absolutely unaware that her daughter had bought a second mobile for herself and was speaking to a stranger.

The imposter called up Sheena's mother and in plain words asked her for 1500 rupees and her daughter failing which he advised her to forget that she ever had a daughter. After the matter was reported and investigation carried out, it was found that actually it was a daily wage laborer using Facebook through his newly bought smartphone.

Recording a child in a sexual activity

i. Mere act of recording, even through a hidden camera

ii. Section 67B(e) of the IT Act applies when abuse of a child is recorded – up to 5 years of imprisonment

iii. Section 66E of the Act also applies- criminalizes capturing, publishing and transmitting image of private part of an individual – Even if some private activity of a child recorded: like changing clothes – up to 3 years of imprisonment

Threatening a child to use his morphed or real depiction in a sexual act

i. Commonly manifests as Sextortion- demand for money or continued sexual favors in return for not publishing

ii. May even lead to Revenge Pornography- when an image/video recorded with consent is published online

iii. Criminalized under Section 11(v) of the POCSO Act and intimidation as per IPC (Section 503) – up to 3 years imprisonment

Case Study: Ahana (Name changed)

It was after one of our pilot workshops in Assam that this case was received from a small town. Ahana is a class 9 student who lives in a small neighborhood. She was being followed by someone constantly for days from her school to her home. This stranger entered her house one day finding her alone and sexually assaulted her to the point of committing rape.

A video of this act was recorded by the culprit and within days, it was being circulated throughout the town. In a few weeks it grew gruesome when the video was uploaded to Facebook and was being shared over WhatsApp. That is when Ahana decided to tell her parents and reach out for help.

Dissemination

i. Publishing, transmitting, causing to be transmitted: Section 67B(a) of the IT Act- up to 5 years of imprisonment

ii. Distribution, Exchanging, Promoting, Advertising: Section 67B(b) of the IT Act

iii. In any electronic form: through direct messaging, public post, upload on a website/portal/forum etc.

Collecting, Seeking, Downloading, Browsing

i. Section 67B(b) of the IT Act – up to 5 years of imprisonment

ii. For merely being found in possession in any form for commercial use: Section 15 of the POCSO Act- up to 3 years of imprisonment

3. Cyber Bullying

Bullying is purposeful, repeated behavior designed to cause physical and emotional distress. Bullying may be physical (hitting, punching, pushing), verbal (teasing, shaming, name-calling, taunting, threatening to cause harm) or social (exclusion from a group, public embarrassment). Cyberbullying (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks. Although Cyber Bullying has not been exclusively defined and penalized under the Indian Law, it is a serious threat that is made up of several activities that are individually criminalized. Some of the activities which may be termed as Cyber Bullying are intimidation and threats, stalking and defamation.

Intimidation and threats	Stalking
i. Threatening to injure his or his family's reputation ii. To make him do something illegal or stop from doing something iii. Punishable under Section 503, 506 and 507 of the IPC: 2 years of punishment + additional 2 years (if anonymous communication) iv. When threatening to use a real or fabricated depiction of a child in a sexual act, Section 11 (v) of the POCSO Act also applies	i. Tracking someone, collecting information about them and their activities despite clear show of interest ii. May be while pretending to be someone else (Cheating) iii. Section 354D, IPC applies to general cases when a man either follows a woman or contacts her despite clear indication of disinterest. Even monitoring behavior through the electronic media is considered stalking iv. But repeated or constant following, watching, contacting a child irrespective of gender is a crime under Section 11(iv) of the POCSO Act- up to 3 years of imprisonment

Case Study on Bullying: Amanda Todd

Amanda Todd was a 15-year-old girl who was blackmailed, bullied, and physically attacked. When she was only 12, she exposed her breasts to a stranger online who took a photograph and then threatened to share it if she didn't "give him a show." However, the stranger still leaked her topless photos which left her vulnerable to bullying. The stranger had her topless photo as his Facebook profile picture and passed it along to her schoolmates. Humiliated, Amanda changed schools, but the picture made it to her new school as well.

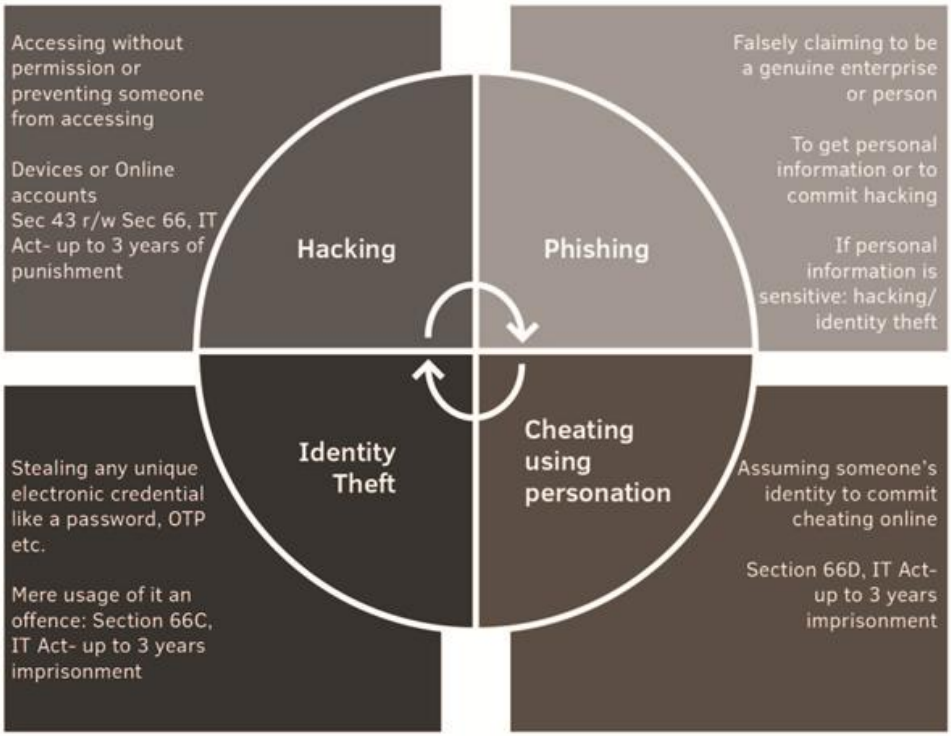
Amanda tried and failed to kill herself by drinking bleach. Her failed suicide attempt only made her more of a target for bullying with pictures of her captioned, "Thirsty? Drink Clorox." To escape the torment, Amanda's family moved; however, the stranger again spread her topless photos around the school by posing as someone who was going to move to that school. Amanda spiraled into a deep depression, posting a video on YouTube detailing the three years of torture, suffering and anguish she had gone through. Months after posting the video, Amanda hanged herself.

Case Studies on Cyber Stalking

An important case on Cyber Stalking is that of State vs Yogesh Prabhu, wherein a girl unfriended the accused but he did not stop following or messaging her. Despite her several requests, he continued sending her vulgar messages and pictures through emails and Orkut. Though it did lead to conviction later on, the case was not exactly filed as a cyber stalking matter because the legal provision was non existent back then.

Another important case is that of Kalindi Charan Leka in the state of Odisha (reported judgment). In this case, the offender, after having his marriage proposal rejected started following the girl both online and offline. He would morph pictures of her and create fake profiles in her name along with pasting pamphlets of those pictures in the hostels that she would live in.

4. Online Frauds



In a recent case, a student of the tenth grade was sent a message on Facebook telling her of how her picture was being used on a pornographic website. She was given a link to the alleged picture which when she opened, asked her for her username and password. The result was that she lost access to her account.

Application of Law

Overriding Effect. It is crucial that the correct law is used while charging an offender of any crime to ensure the right procedure for trial. For sexual offences against children, it must be noted that under Section 42A of the POCSO Act, it has been laid down that provisions of the POCSO Act are in addition to the provisions of other laws and not in derogation of them. However, when there is an inconsistency between POCSO Act and other laws, POCSO Act will override them. Hence, in cases like Cyber Stalking and Criminal Intimidation in the POCSO Act, where there is a corresponding provision of the same nature in the IPC as well, the provisions of POCSO Act will have overriding effect.

Mandatory use of IT Act. The IT Act is a special provision for cyber offences and hence, it must be used in all cases of cyber crimes. Therefore, whenever there is a remedy under the IT Act for an offence against a child, the IT Act needs to be used if not exclusively, then in addition to the provisions of the POCSO Act or the IPC.

Different quantum of punishments. It might also be possible in certain cases that the same offence listed under the POCSO Act and IT Act has different quantum of punishment in both the legislations. In such a case, one should must use both the provisions but it should be ensured that the one with more punishment is compulsorily added. For example, the offence of enticement of children only warrants a

a three year punishment under Section 11 of the POCSO Act while it warrants a five year punishment under Section 67B of the IT Act.

Bailability. It is also important to know that if the investigating officer fails to apply all relevant laws to a particular situation, problems of bailability may also arise. Under the IT Act for example, as all offences with punishment up to three years are bailable, if the IO misses out on applying another provision to make the charges non-bailable, the offender can be out on bail as a matter of right and then destroy evidence or tamper it which is a very common activity in cases of cyber crimes.

Offence	IPC & POCSO Act	IT Act
If punishable with imprisonment for 3 years	Cognizable and Non-Bailable	Cognizable and Bailable

Consent. All sexual acts described under POCSO Act are, without exception, considered to be criminal offences when the victim is under the age of 18 years. This holds true regardless of the issue of consent. As for provisions of the IT Act like Section 66E which criminalizes the act of capturing/publishing images of private areas of any person without their consent, a child's consent cannot be an excuse/validation of the act.

What happens when the perpetrator is a child?

Undoubtedly, a person doing any of the activities listed under the last sections may be an adult or a child. In situations where a child is the perpetrator of the criminal activity, he/she needs to be dealt with as a Child in Conflict with law as per the provisions of the Juvenile Justice Act and not in a manner an adult would be treated. For cases even under the POCSO Act, Section 34(1) lays down that when any offence is committed by a child, such child shall be dealt with under the provisions of the Juvenile Justice Act. Therefore, provisions with respect to dealing with a child in conflict with law must be looked at from the Juvenile Justice Act.

- As per Section 107 of the Juvenile Justice Act, a Child Welfare Police Officer (CWPO) at each police station (who is not supposed to be below the rank of a sub-inspector) may be designated to deal with children specifically who is supposed to be the medium between the victim/perpetrator child, police, welfare committee or juvenile justice board as the case may be and any voluntary/government/non-governmental organization.

- The officer apprehending a Child in Conflict with Law has to report and place the child under the charge of Special Juvenile Police Unit or the Child Welfare Police Officer within 24 hours as per the requirement of Section 10(1) of the Juvenile Justice Act.

- Such a child is never to be placed in a police lockup or jail. Before being produced before the Juvenile Justice Board, the child is to be placed in an observation home.

- The Juvenile Justice Board formed under the Act is empowered to hold inquiries into matters involving children in conflict with law.

- When the nature of a crime is not heinous (that attract a punishment of seven years or more), or when heinous and the child is below the age of sixteen years, the board proceeds as per general provisions of the Act.

- A child found in conflict with law who has committed a petty offence, a serious offence or if a child below age of sixteen years has committed a heinous offence is dealt with as per Section 18 of the Act and he may be either allowed to go home or be released on probation, required to participate in group counseling, ordered to perform community service or be sent to a special home but not for more than a period of three years etc.

- In heinous cases and when the child is above sixteen years of age, a preliminary inquiry is held by the board to assess the mental and physical capacity of the child to commit the offence in accordance with Section 15 of the Act. If he/she is found capable, the board is to follow the trial procedure as in a summons case under the Code of Criminal Procedure as would normally apply to an adult.

CYBER PEACE FOUNDATION

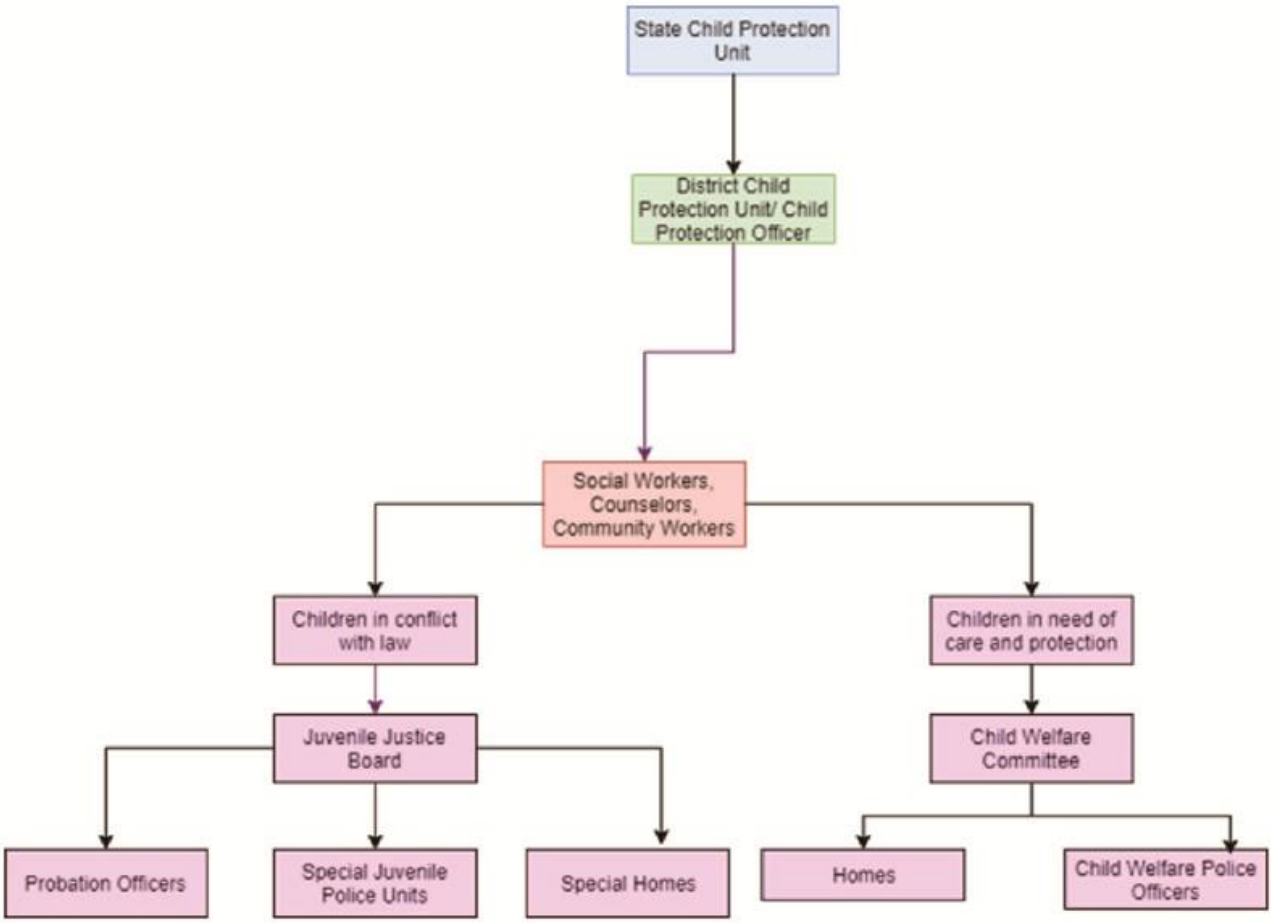
unicef
for every child

PART - II

Guidelines for Law Enforcement Agencies

Child Protection Infrastructure in India

The Juvenile Justice (Care and Protection) Act and the Protection of Children from Sexual Offences (POCSO) Act protect all children under the age of 18 years from procedural hassles in cases of offences done by and against them. Several authorities have been set up under the Juvenile Justice Act, namely Special Juvenile Police Units, Child Welfare Committees, Juvenile Justice boards, Special Homes etc. An Integrated Child Protection Scheme has also been set up to bring all these functionaries of child protection programs under one umbrella. It is a Government-Civil Society partnership scheme which is aimed at facilitating adequate child protection services delivery in line with the state objectives. State Child Protection Societies (SCPS) and District Child Protection Units (DCPUs) have been set up under the scheme as fundamental units for implementation at State and District levels respectively.



Two categories of children have been identified under these laws: Child in Conflict with Law (CCL) and Child in need of care and protection (CNCP). While CCL may refer to a child who has or is alleged to have committed an offence as per Section 2(13) of the Juvenile Justice Act, CNCP covers all children requiring state care and protection and has an inclusive definition which has been given under 2(14) of the Juvenile Justice Act referring to a child who has been abandoned, orphaned, found without a home, residing with a possible perpetrator etc.

Receipt of Complaint

While, receiving a complaint or responding to a cyber crime against a child, some guiding principles which a police officer should make note of:

1. An offence against a child may be reported by anyone. In fact, any person who has an apprehension or knowledge of an offence against child is required to mandatorily report about it to the police under Section 19(1) of the POCSO Act. There is a specific compulsion upon media houses, studios and photographic facilities to report cases of Child Sexual Abuse or about any material or object which is pornographic or obscene and sexually exploitative of the child. Failing these mandatory reporting requirements, an imprisonment of a term of six months may be imposed upon the defaulters as per Section 21 of the POCSO Act.

2. Upon receiving a complaint, it is the duty of the police officer receiving such complaint to register an FIR in accordance with the instructions given under the POCSO Act. In case of failure in recording this report, a police officer is liable for a punishment of imprisonment for up to six months as per the provision of Section 166A of the IPC. A police officer may also be punished with imprisonment for a term of six months in case he fails to record a case as per the requirements of Section 19 of the POCSO Act.

3. As per the POCSO Act, a police unit is required to maintain an entry book in which every report shall be ascribed with an entry number and recorded in writing. Thereafter, it shall be read in verbatim to the informant. (Section 19(2)). In case there is a language barrier, a translator or interpreter should be arranged for. (Section 19(4))

4. While responding to even a cyber crime, you may find or be handed over a child who appears or claims to be an orphan and without family support. This may happen when you are visiting a scene or while gathering preliminary information. In such a case, you are bound to give information to either the Childline services, nearest police station, CWC or the DCPU and hand over the child to the nearest Child care institution registered under the Juvenile Justice Act within 24 hours (Section 32). This responsibility has also been placed on functionaries of any organizations, nursing homes, hospitals and maternity homes. If a person fails to mandatorily report under this provision, it can attract punishment of imprisonment for up to six months. (Section 34)

Tell the parents

- To save screenshots/URLs/messages/multimedia files etc. that may act as evidence
- To talk to the child and ask not to disclose any personal information like home/school address
- To ensure that the child from does not deactivate/delete accounts or communication with the offender
- To notice changes in the child's behavior and get expert help if needed

5. If a matter appears to be such that the provisions of the POCSO Act need to be applied, the procedures of the POCSO Act need to be adhered to over other laws. Section 19(5) of the POCSO Act mandates that that when the police are satisfied that a child victim is in need of care and protection (for example, child has no parents or relatives to go to, has been living, he/she shall be admitted into a shelter home or the nearest hospital within 24 hours of receiving report about such a child. Reasons for the response have to be recorded in writing. As per Section 19(6) of the Act, the police must also report the matter to the Child Welfare Committee and the Special Court without unnecessary delay, but within a period of 24 hours. (If no special court is designated, then the Sessions Court)

6. If apprehending a Child in Conflict with Law, the police officer has to report and place the child under the charge of Special Juvenile Police Unit or the Child Welfare Police Officer within 24 hours as per the requirement of Section 10(1) of the Juvenile Justice Act. Such a child cannot be detained in a police station or placed in a jail or lockup at any cost.

7. The CWPO is required to coordinate with all functionaries involved in dealing with a case involving a child. Therefore, at all times, the officer investigating and interacting with a child must keep the CWPO updated about all developments.

8. The IO should either go to the victim's house or ask for a convenient place of meeting for recording of statement and the recording of statement should be preferably made by a woman officer not below the rank of sub-inspector. (Section 24(1), POCSO Act)

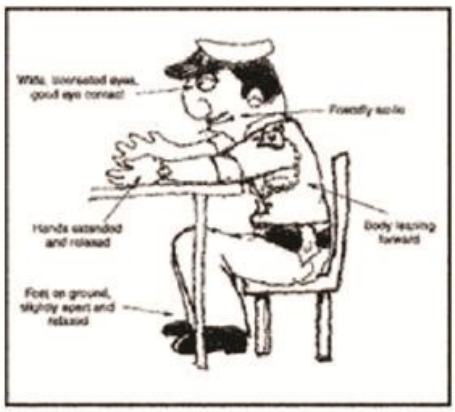
9. The officer recording the statement should not be in uniform. (Section 24(2), POCSO Act)

10. A child can also not be detained in a police station at night for any reason (Section 24(4), POCSO Act). It should also be ensured that the accused is not in contact with the child at any point during the investigation (Section 24(3), POCSO Act) and that the child's identity is kept a secret unless ordered by the Special Court (Section 24(5), POCSO Act). A punishment of six months of imprisonment in case of disclosure is also prescribed (Section 74, Juvenile Justice Act)

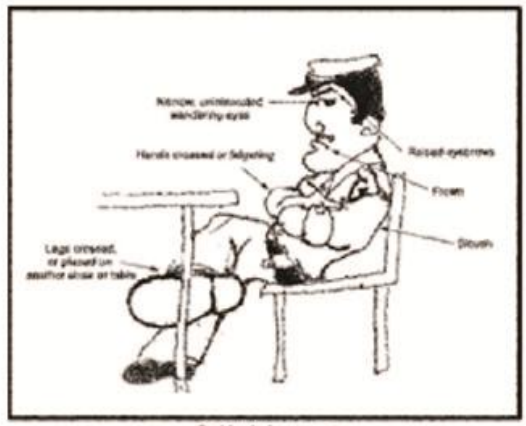
11. As per the mandates of the POCSO Act and Juvenile Justice Act, a police official must cater to a child in need of care and protection and one in conflict with law. You must ensure that the child is getting proper care and is not a victim of any further exposure. There are many organizations both state as well as non-state working in the domain of providing care. You can get in touch with the District Child Protection Unit and find a suitable organization for expert help and care. Follow this link for details of all DCPUs in the country: http://carings.nic.in/caraHQ/DCPU_Detail_Online.aspx

12. No report in any newspaper, magazine, news-sheet or audio-visual media or other forms of communication regarding any inquiry or investigation or judicial procedure shall be published which may lead to identification of a child be it an offender or a victim. Any person disclosing any information about the child may be punished with imprisonment for up to six months (Section 74(3), Juvenile Justice Act). Under the POCSO Act as well, name, address, photograph, family details, school, neighborhood or any other particulars which may lead to disclosure of identity of the child cannot be published in any manner (Section 23(2)), the punishment which is not less than six months of imprisonment but which may extend to one year. (Section 23 (4))

13. Your body language can be very expressive sometimes. Make sure that whenever you talk to the victim, you must sit or stand properly and treat the victim and the family with respect. It will also help to go back to the section on "Why is sensitization important" at this stage to understand the nature of children more closely and be better prepared to interact with a child. An "I know" approach will not be relevant in such cases, instead you should make the victim feel that you really want to know.



Good Body Language



Bad body language

Karnataka State Police- UNICEF Training and Resource Manual for Police Personnel 2003

Pre Investigation

A pre-investigation assessment helps the IO narrow down the entire factual situation of the offence and decide what must be done immediately. During Pre Investigation, an IO will see whether there is needs to seize any device for forensic examination, send out certain notices etc. At this stage in the investigation, the IO should list down important things like:

a. The exact offence in question, corresponding to its law
b. Available evidence (Images, Messages, IP Addresses, Emails etc.)
c. Modus Operandi of the criminal
d. Social Media or other Service Providers involved
e. Build a timeline based on the victim's account and the available evidence

Modus Operandi as opposed to a crime involving an adult

In case of a crime against an adult, an Investigating Officer would generally look for communication on Chat messengers, Emails and Social Media etc. When investigating a similar crime against a child, chances are that one might miss out on important other places where communication is possible, a game chat room for example. It has been often found that children are bullied and harassed while playing games, in chat rooms etc.

In cases of cyber crime, an IO may or may not find a physical scene of crime. A physical scene in a cyber crime could be anything ranging from a perpetrator's house with his laptop or a cyber café or server room with complex networks. In such a case, the IO must visit the scene of offence and photograph/videograph the entire scene in the "as is where is" manner. If the IO is not an expert in technology and the scene of crime looks complex, he must take help of a forensic specialist to seize evidence and transport it.

When there are no devices with the victim and the criminal is unidentified (meaning no physical scene of crime), the police need to rely on data from service providers as evidence and conventional witnesses to solve the crime. In such a case where there may only be data from service providers, the IO need not seize and transport evidence as has been discussed ahead but will still need to interview all relevant people like the child's parents, school friends, social media friends etc. to gather evidence and establish timelines. A simple situation when there is going to be nothing to forensically examine is when a child is being threatened on social media and the only credible evidence to locate the criminal would be the account data sent over by the social media.

The potential evidence after being properly seized is sent to a forensic laboratory for further testing. While there may not be an exhaustive list of things to do, some things that need to be taken care of:

- Remove all persons from the scene of crime
- Ensure that no unauthorized person has access to the devices at a scene
- Refuse any technical assistance from anyone on scene except recognized forensic specialists
- It is recommended to photograph the entire scene of evidence and also draw connections wherever they exist
- When a device is switched on, it should be left as it is and if it is switched off, it should not be switched on for investigation
- If it is a mobile device, make sure to put it in the flight mode (Not switched off) for transportation as it will prevent any communication from the offender remotely
- Document any activity on screen the moment you arrive
- Videograph the entire scene of crime and any additional activity that you may do on the original system to log and establish any change that forensics might later reflect
- If the officer has to seize the evidence himself, he must make use of Faraday bags or other such electro magnetically safe containers

Potential Sources of Electronic evidence

Digital Devices	Storage Devices	Hand Held Devices	Other
Desktop	Hard Drive	Smartphones	Router
Laptop	CD, DVD and Blu Ray	Tablets	Switch
Server Rack	Memory cards and OTG devices	Smart watch	Hub
	Flash Drives	IoT Devices like Smart plugs and bulbs	Home Automation and Voice Assistants, Robots etc.
	Memory Sticks	Health Tracking Devices	Telephone
	Printers and Scanners	Telephone	Answering Machines
	Network Attached Storage (NAS)	Satellite Phones	Camera and Recorders
			GPS Devices

Handling Evidence

Electronic or Digital Evidence is that type of information which is either stored, created or transmitted in the electronic form, meaning through computer resources. It is naturally one of the most fragile and vulnerable forms of evidence. While collecting and retaining electronic devices for evidence during investigations,

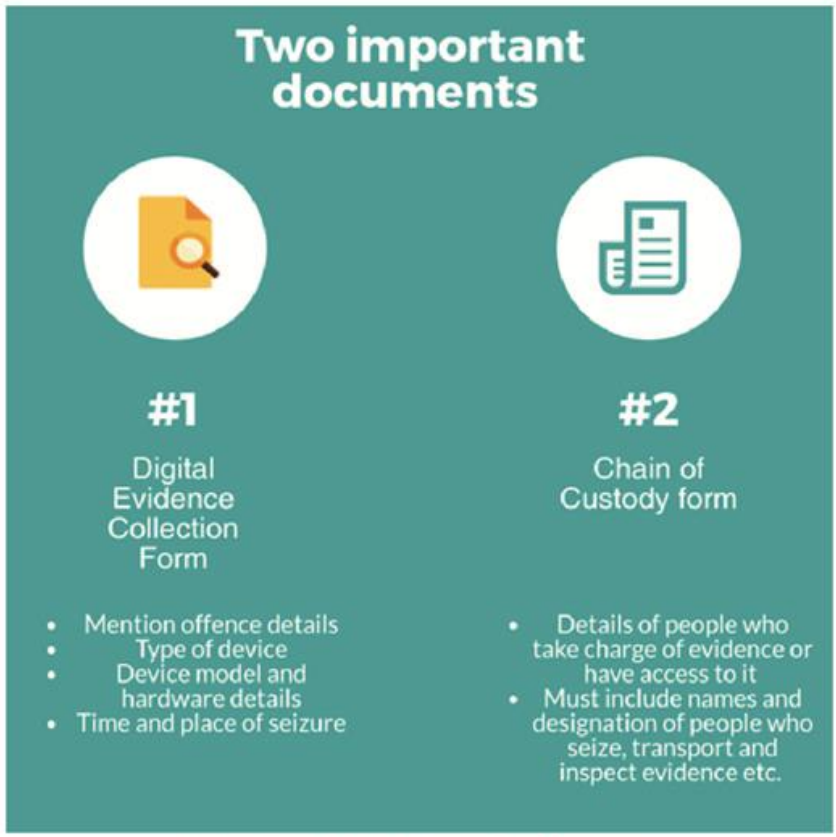
a. The IO must obtain the competent court's order to retain the seized properties for the purpose of investigation.

b. The IO must also obtain the court's order to send the acquired properties for forensic analysis and expert opinion.

c. The IO must also chalk out the objections to be raised in case the owner of the property applies to the court for reclaiming the possession over such seized properties.

Subsequently, it should also be noted that the officers should not perform any operation on the principal device, i.e. the mobile phone, router, tablet or PC etc. because it can potentially alter contents of the device and cause a problem in admissibility during trial.

There are two critical documents at the stage of evidence collection, namely the Digital Evidence Collection and Chain of Custody form.

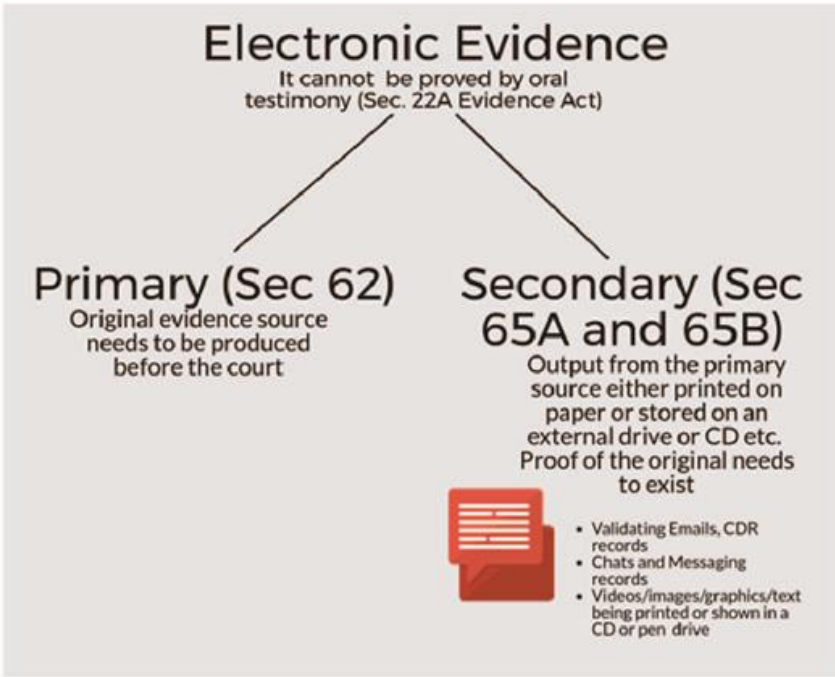


Please refer to Annexure I for formats

There is moreover a liability on the IO to protect and keep the information contained in the evidence unrevealed. As per Section 72 of the IT Act, if an IO in his officiating capacity discloses the contents of an evidence to another person without the consent of the person concerned, then it attracts a punishment of up to 2 years with fine extending up to one lakh rupees

The general practice in prosecution is that the defense challenges the integrity of the evidence claiming it to be tampered. At such an instance the electronic evidence collection and chain of custody documents play a vital role in proving the genuineness of the evidence.

Admissibility of Electronic Evidence



While primary electronic evidence or evidence in its original form with the device used to create it may be proved in court as per Section 62 of the Evidence Act without the need for any additional document, secondary evidence needs to be proved with the help of a special certificate. When any document is adduced in court as a print out or reproduction on a storage media like a printed Email conversation or recorded video clip in a CD, the requirements of Section 65A and 65B need to be fulfilled.
Sec 65B (2) specifically lays down the prerequisites that need to be satisfied for secondary evidence to be admissible. To summarize, these are:

a. It should be output of time during which device was being used regularly for regular purposes by person exercising lawful control over the device. Such output should have been result of regular feeding of data in ordinary course of the activity.

b. The device was working properly and even if it was not then it should not have affected its accuracy.

c. That the information being produced is either the reproduction of or derived from such information as fed into the device in ordinary course of activities.

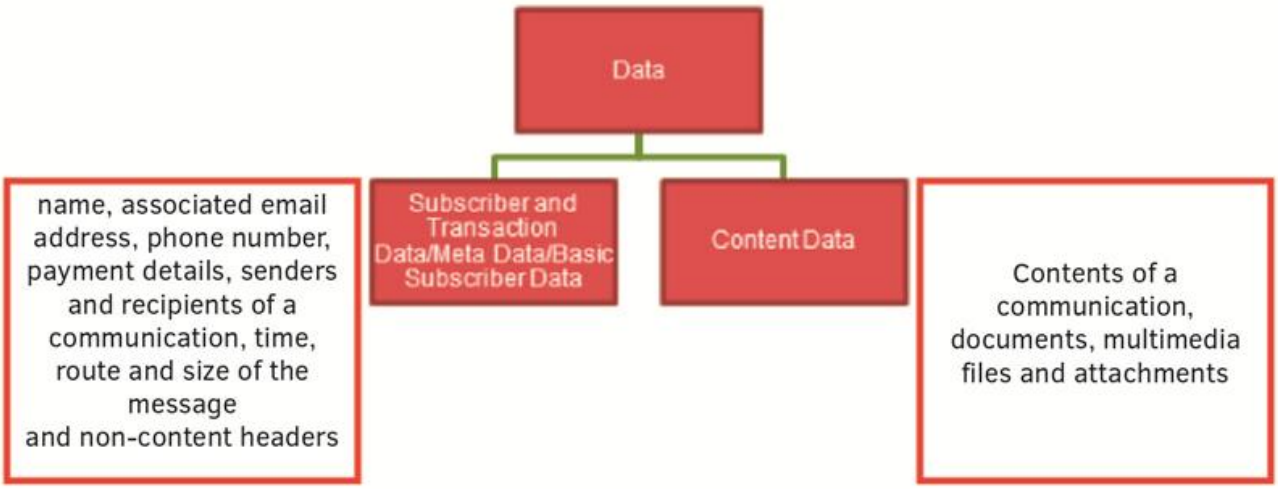
As per the requirement of law, a certificate stating the above and with the particulars of the device involved in production of the evidence has to be given by a person occupying a responsible official position in relation to the device. As of now, forensic laboratories and electronic evidence examiners have been designated to certify with respect to electronic evidence. With respect to screenshots and printouts of information from personal devices, it has been observed that the owner of the devices give this certificate through an affidavit. It is suggested that the IO should consult with the prosecuting officer on the case to verify the local format and manner of submission of Section 65B certificate. It is because without this certificate of admissibility, secondary electronic evidence is not admissible.

Investigation

During an investigation, an IO needs data to continue investigation and to record his findings. This data may be in the form of IP addresses, logs, registration details, mobile numbers, addresses etc. which is usually with service providers. These service providers may be telecommunication companies like BSNL, Vodafone etc. or websites, portals, payment gateways etc. operating out of India that share data with law enforcement easily. However, some of these major service providers to the Indian citizens are International like Facebook, WhatsApp, Google etc., whose data is stored abroad, so a specific set of procedures needs to be followed in order to get the required data from them.

1. Data Requests and Notices

There are 2 different types of data broadly that have been described as under:



There are different processes to get both these types of data. Conventionally, there are three different types of procedures to get data from service providers: Direct Requests, MLAT requests and Letters Rogatory. While Direct Requests and MLAT requests may fetch the Subscriber/Transaction data, the actual contents of a communication may be given by a service provider only through a Letters Rogatory request.

Direct Request (Section 91 CrPC Notice)

An IO can generally send a request under Section 91 of the CrPC to compel the production of a "document or a thing." Under this section, a police officer only needs to produce a written request to access data when it is considered "necessary or desirable" for an investigation or trial. But it has to be strictly observed that only non-content data requests are made. In case of a crime against a child, a data request can be treated as emergency if an IO specifies how there is eminent and unavoidable threat to the child. When such a request is made, most of the service providers comply within hours of receipt. Some services even provide 24x7 assistance including some pornographic websites.

Generally, every service provider will have different law enforcement guidelines which need to be complied with in order to get some data, so an officer should exhaustively factor in all the guidelines and then draft a notice.

A notice under Section 91 may contain one or both of the following:

- **Data Request Notice:** Notice to request production of data about a profile/user account, IP address etc.
- **Data Preservation/Retention Notice:** Notice to require retention of data while investigation is pending.

In India, the IT Act under Section 67C imposes a liability upon service providers to retain data for fixed time spans. In some cases, like ISPs, commercial billing records need to be stored for a period of at least one year. For service providers like websites and apps however, there is no time specification. As for the United States law, there is a provision requiring companies to preserve data for 90 days upon receiving a request to retain.

What an officer needs to ensure while sending a Section 91 notice to any service provider:

a. Must be sent from the Official and authorized government Email ID and on the agency's letterhead.

b. Must highlight that it is an urgent request for a crime against a child.

c. Must contain the FIR number (as FIR is mandatory for crimes against children)

d. Must list down all the details being sought.

e. Must contain the name and rank of the IO.

f. Must contain a brief of the offence constituted and the legal provisions in India making such act a crime.

g. Must contain a preservation request if needed.

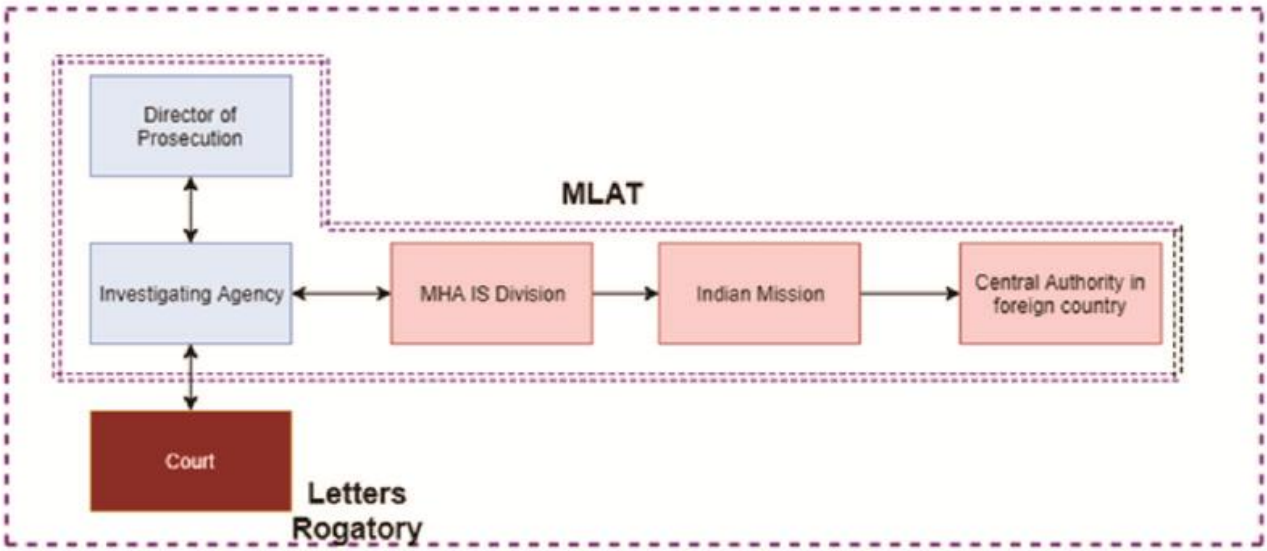
Challenge in Investigation	Solution for crimes against children
Long turnaround or response time by service providers	When provided by service providers like Facebook and WhatsApp, use special emergency request route for data requests. Mention the nature and reason for emergency in the Section 91 notice. Usually providers reply within hours to such requests
Data lost or deleted by the user or service provider by time investigation completes	Data Preservation Request to store important data during the course of investigation. Even if offenders delete the account, this request will save its data
Accounts or data is on explicit/pornographic websites	Even pornographic websites have a zero tolerance policy for crimes against children. Some porn websites even have a 24x7 assistance channel for crimes against children

MLAT & Letters Rogatory

MLATs (Mutual Legal Assistance Treaties) & Letters Rogatory are two formal tools through which law enforcement agencies can seek assistance of foreign law enforcement agencies and courts during criminal investigations. State police agencies and CBI make use of Letters Rogatory when direct notices do not generate any result. Agencies like the NIA on the other hand make use of MLATs. A mutual legal assistance treaty is generally a bilateral agreement entered into by countries to exchange evidence and to serve summons etc. during criminal investigations and prosecutions involving persons of non-domestic nationality. MLATs do not require the assent of a court in order to function. Letters Rogatory on the other hand, is sent by a Criminal Court on request of an IO or other officer of a higher rank to a court of another country requesting the necessary data, evidence include oral testimony of a person that is within that country. The designated central body for routing a both these types of request is the Ministry of Home Affairs.

While there may be different arrangements like the MLATs with different countries, the most relevant for the purpose of investigation is the India-USA MLAT. As most of the service providers and their headquarters are based in USA, they would require the USA legal process for law enforcement requests to be followed. The good thing about the US-India MLAT is that it does not pose a dual criminality requirement, instead it requires the subject of investigation to be a crime in the requesting country only. But this does not mean there may not be any arrangement with other countries at all.

India has so far entered into MLATs with 39 countries, the terms of each MLAT being different. The scope of the MLAT includes execution of searches, seizures and provision of documents, records and items for evidence. India has currently entered into MLAT with 39 countries.



2. How Service Providers interact?

It becomes very important to know and understand the kind of data that can be fetched from various sources under these notices and data requests.
Internet Service Providers/Mobile Service Providers

- User Details
- Call Data Record
- Tower data and location
- IP Details such as IP allotted to a user at a particular instance
- Mobile/Telephone number
- Day wise activity (Duration of usage, size of download/upload)
- Call Data Record, SMS billing history
- Tower data and location
- Roaming Details
- Specific IP Details

Email Service Providers

- Username
- IP Address using which the account was created, date and time of creation and alternate email id
- IP Address used to send a particular email
- login, logout and session time
- All communication between the criminal and victim using particular email id including the one in draft.
- Google has a dedicated portal for law enforcement agencies which handles requests for all Google products, so it will be applicable for Gmail, YouTube, Google Docs

and G+ etc. as well. The portal can be accessed using an official email id at https://lers.google.com/signup#/landing. Most other email service providers have dedicated portals or communication mechanism to receive and process by LEA.

Social Media

Generally, all Social Media companies store different types of Data and in a different manner. An IO can search online for Law Enforcement Guidelines for a specific social media and follow them for getting the required data. The major out of the many have been discussed:

- **Facebook:** Facebook has a dedicated portal for law enforcement requests which is available at https://www.facebook.com/records/x/login/. An IO needs to login with his official Email ID on the portal and would need to lodge a request for data there along with the proper Section 91 notice as described earlier. An IO can make emergency requests citing matters involving children because Facebook has a special policy for crime against children. An IO can also make a data preservation request which lasts for 90 days. A detailed guide by Facebook for law enforcement agencies is available at https://www.eff.org/files/filenode/social_network/facebook2010_sn_leg-doj.pdf.

- As per the Law Enforcement Guidelines by Facebook, IO needs to be submit the email address, user URL (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile. Details of the content that Facebook may share with Law enforcement has been appended in Annexure V.

- **WhatsApp:** Like the parent company Facebook, WhatsApp also participates in the Law Enforcement support processes. For WhatsApp, there is no dedicated portal however. Requests for Data and Data Preservation need to be forwarded to records@whatsapp.com with the mobile number clearly stated with respect to which data is being sought. Many traditional crimes today that happen offline as well need data from WhatsApp as the active user base of WhatsApp in India is huge. The jurisprudence since the end to end encryption feature on WhatsApp in very minimal, but it is known that in the United States, even pen tap orders have been issued against users on WhatsApp. However, WhatsApp denies storing any sort of communication including images because of the end to end encryption. However, it stores and shares:

a. When was account created
b. Date of last opening
c. Device
d. Network through which account was accessed d
e. Webpages visited through WhatsApp
f. IP addresses of account creation and usage
g. Other apps accesses via WhatsApp : like Google Drive for WhatsApp
h. Groups
i. Address Book
j. Size of Messages and duration of chats etc

- **Twitter:** Similar Law Enforcement Relationship Management portal for Twitter is available at https://legalrequests.twitter.com/forms/landing_disclaimer. In furtherance of this, the guide lines for law enforcement are available at https://support.twitter.com/articles/41949.

- Skype: Skype is both a Social Media Service and a VoIP service. Its policy for Law Enforcement agencies is available at https://cryptome.org/isp-spy/skype-spy.pdf

- YouTube: All requests need to be made via Google's law enforcement portal at https://lers.google.com/signup#/landing. YouTube also has a special policy against child endangerment which means they would escalate an urgent request involving a child. YouTube can also be reached by Law Enforcement agencies via legal@support.youtube.com

- SnapChat: Snapchat's law enforcement policy is available at https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf

Websites

For individual websites, an IO can find out the email ID dedicated for data requests and follow the same procedure as above. In case, there is no such designated email address, then the IO can send to any such communication email listed on the website. Alternatively, the request can be sent via Post as well. Even major pornographic websites have zero tolerance for hate crime and crimes against children, so an IO should not refrain from sending out notices to such websites also in case they host content or can be possible sources of evidence. The difference in the request here would be in the kind of things being asked for, they include:

a. Owner of website
b. Details of a specific user on website
c. Details of specific content hosted on website (Who uploaded, from where, IP address)
d. Access logs of the website (depicting IP addresses)
e. Details of website developer etc.

When there is an unknown service provider

It might be possible that a service one comes across is totally new and has never come up during investigations before. When data is needed from such service providers, an IO should search the internet for the service provider's law enforcement guidelines document to know the process that they follow and the manner of contacting them. For this, an IO can simply search the Internet through any search engine for the guidelines. Such searches would generally lead you to a dedicated page or a document that has all details about legal processes and the information needed in order to process a data request.

3. Locating the Criminal

Most likely, a notice is going to yield a set of details about a user and his activity. In addition to the other details as mentioned in the previous sections, this will lead to an IP address as well. It has been found through research that most of the officers are aware of and have been tracking offenders through IP addresses. For the sake of continuity, however, some important things have been mentioned here. It must be noted that IP addresses are generally dynamic, so there are time slots for which IP Addresses are allotted and then reallocation keeps taking place. One IP address might be allotted to 10 different people during the entire day. However, one IP is assigned to only connection at one single point of time. The IO can then search for the name of the Internet Service Provider (ISP) of the specific IP through tools available on websites like *www.viewdns.info.*

At this stage:

• Note the IP Address and other details received from the Communication Service Provider.

• Make sure to change the time zone format from let us say UTC to GMT+5:30 in case the ISP is located in India.

• A tool for executing this is available at https://www.timeanddate.com/worldclock/converter.html.

• Draft a fresh Section 91 CrPC notice for the concerned ISP to furnish desired user details about the specific IP in the time slot mentioned and possible subscription form details. (Mentioning that the request is in relation to a crime against a child will expedite the process of response here as well)

• The ISP sends back the details as desired and mentioned in the which may then be corroborated with other evidence to conclusively narrow down the offender.

Final Report

1. Preparing the Charge Sheet

Slackly prepared charge sheets are a reason why several criminals escape the law. It is important for the IO to ensure that there is no benefit of doubt in favour of the criminal which allows him to bypass the law. Important markers to be included in the final report while preparing charge sheet:

- Information shared by the victim at the time of filing an FIR
- Provisions of Law; The IO should also ensure that charges framed under various provisions of law are not repealed or amended. Several cases till day are being filed under Section 66 A of the IT Act which was repealed in 2015
- Detailed information of crime scene which the IO visited
- Detailed information of each evidence collected from the crime scene and manner of collection
- Chain of custody form of each evidence collected from the crime scene and otherwise which helps prove before the court of law that the evidence is not tampered with
- Report of Forensic Examiner(s), if any
- Time Line of the entire procedure of investigation beginning from the time the crime occurred.

All the crucial evidence must be stored until produced before a court of law. All the devices must be numbered and kept in antistatic fireproof bags to avoid any loss of data. The bags should then be stored in a cool dry place beyond the reach of any ordinary person.

- Since in practice Section 65B certification is different in different jurisdictions, the IO must consult the prosecutor to ensure that admissibility standards are being met.
- For whatever reason if the device is taken out again before being produced in court, the chain of custody must be updated. No leniency can be shown while dealing with electronic evidence, as even a single loophole can put to question the credibility of the evidence leaving the criminal to walk out freely.

As for POCSO Act as already mentioned, when there is any provision in any other law that is inconsistent with the POCSO Act, then the POCSO Act has overriding effect according to Section 42A. Therefore, when there is criminal activity against children and its remedy is available under the POCSO Act, it should be used exclusively. Non-application of a special law to avoid procedural hurdles will only lead to complications later at the stage of prosecution. As per the recent Supreme Court judgment in the case of Sharat Babu Digumarti v Govt. of NCT of Delhi(2016), the IT Act also has been held to be a special provision, so it must have special effect as well. Generally, if a person is absolved of a crime under the IT Act, similar proceedings under the IPC hold no good. Therefore, when a remedy under the IT Act is available, it shall also be used in addition to the POCSO Act.

Annexes

Annexure I
Electronic evidence Collection Form

Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	

Computer Information			
☐ Laptop	☐ Desktop	Manufacturer	
☐ HDD Only	☐ External HDD	Model Number	
☐ Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	

Courtesy: Cyber Crime Investigation Manual by DSCI

Chain of Custody Form

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number..... Date of Seizure.....

Name of the I.O..... Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Courtesy: Cyber Crime Investigation Manual by DSCI

Annexure II
Sample Notice Under S.91 CrPC

Courtesy: Cyber Crime Investigation Manual by DSCI

From: Name of the Investigating Officer or Supervisory Officer (Police Inspector or above) Provide Full address, phone number and Official Mail ID.		Place Date

NOTICE UNDER SECTION 91 CrPC

To,

The Manager
ABC Company
ISP Division, Mumbai.

Sub: Request to furnish the details about the IP address.

Ref: Crime Number: xxxxxxxxxx u/s xxxxxxxxx of ITAA2008 of xxxxxxxx Police Station, xxxxxxxx City / District

With reference to the above cited subject, the undersigned is investigating officer of the criminal case mentioned above. For the purposes of investigation, details of the subscriber and his/her physical address details are required as per below mentioned IP addresses.

203.94.218.220 on 07 Feb 2008 at 05:01:24 pm GMT (22:31:24 in IST)

Please treat the matter as most urgent.

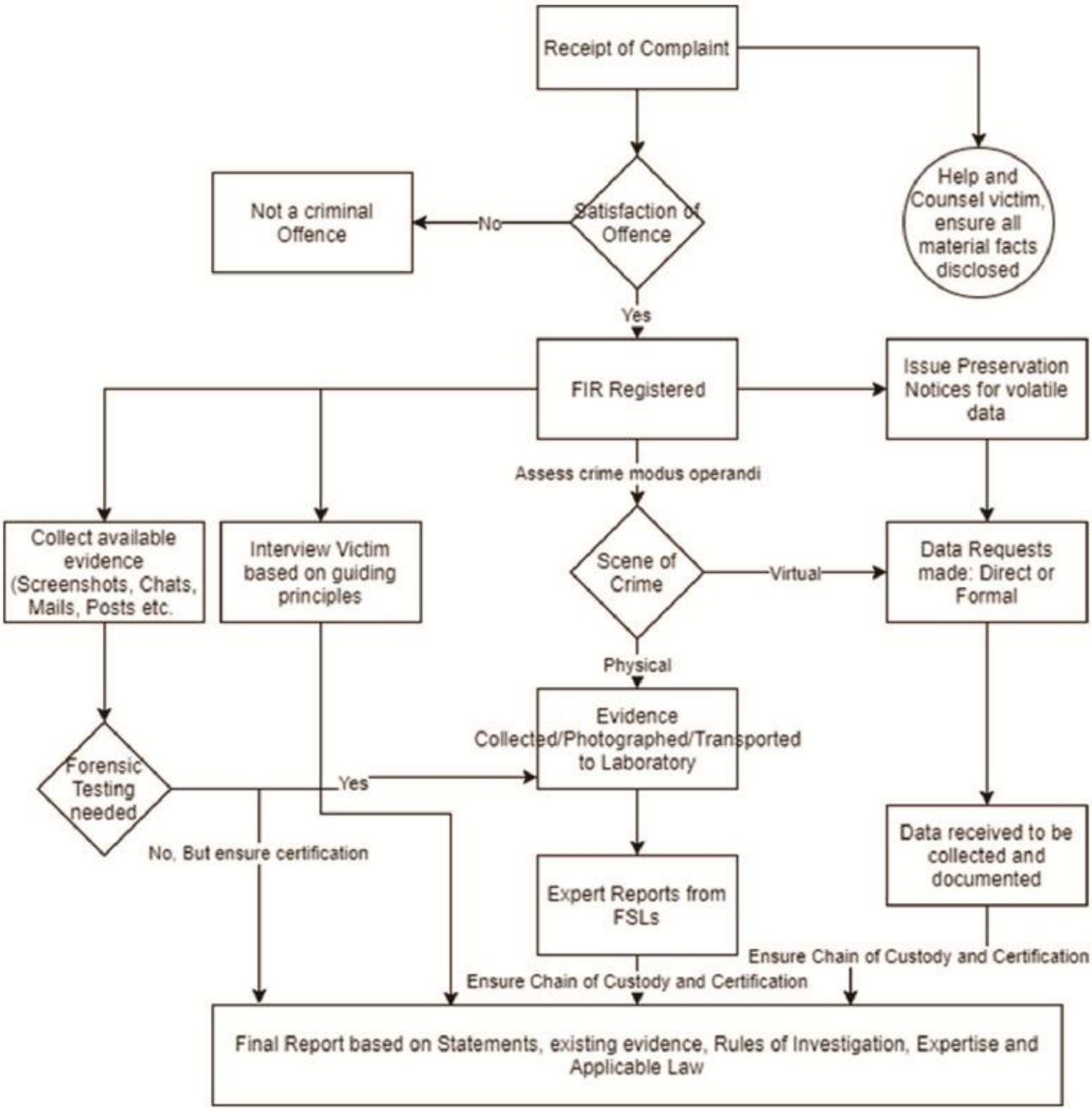
Official Seal	(Signature of the Investigating Officer or Supervisory Officer Demanding Information)

Annexure III
List of Criminal Activities

Activity	Law
Penetrative Sexual Assault	Sections 3 & 4, POCSO Act
Aggravated Penetrative Sexual Assault	Sections 5 & 6, POCSO Act
Sexual Assault	Sections 7 & 8, POCSO Act
Aggravated Sexual Assault	Sections 9 & 10, POCSO Act
Sexual Harassment	Sections 11 & 12, POCSO Act
Writing/Sharing or causing any activity to outrage a woman's modesty	Section 509, IPC
Threatening to use a real or morphed depiction of a child or his body part via any medium in any sexual act	Sections 11 & 12, POCSO Act Section 292, IPC
Saying anything, making any sound or gesture or exhibiting any object or body part with a sexual intention	Sections 11 & 12, POCSO Act
Sending anything lascivious (revealing sexual interest) to a child or showing him anything to corrupt his mind	Section 67, IT Act
Threatening to injure reputation and causing any illegal act to be committed	Section 503 and 506, IPC Section 292, IPC
Cultivating, enticing or inducing children into online relationships	Section 67B, IT Act Sections 11 & 12, POCSO Act
Use of child in any form of media for sexual gratification including just representation of his sexual organs, his engagement in a sexual act (whether real or not, whether with or without penetration) or any indecent or obscene representation of a child	Sections 13 & 14, POCSO Act
Publication or transmission or causing to transmit child pornography	Section 67B, IT Act
Creating, Collecting, Seeking, Browsing, Downloading, Promoting, Exchanging, Distributing or Advertising child pornography	Section 67B, IT Act

Creating, Collecting, Seeking, Browsing, Downloading, Promoting, Exchanging, Distributing or Advertising child pornography	**Section 67B, IT Act**
Recording any child pornographic content	Section 67B, IT Act
Making a child exhibit his body or any part of his body with a sexual intent	Section 11 & 12, POCSO Act
Enticing a child (luring him) for pornographic purposes	Sections 11 & 12, POCSO Act
Showing any object to a child in any form with a sexual intent	Sections 11 & 12, POCSO Act
Facilitating abuse of children online	Section 67B, IT Act
Capturing, publishing or transmitting image of private area of a child	Section 66E, IT Act Sections 13 & 14, POCSO Act Section 354C, IPC

Annexure IV
SOP for Cyber Crime Investigation



Annexure V
Details and Types of Data for a standard Facebook Response

Types of Data

Depending on the type of formal legal process provided, we will be able to respond with one or more of the following types of data:

Basic Subscriber Information (sometimes referred to as Neoselect) will be delivered in XML format and may include:

- User Identification Number
- E-mail address
- Date and Time Stamp of account creation date displayed in **Coordinated Universal Time**
- Most Recent Logins (generally captures the last 2-3 days of logs prior to processing the request) in **Coordinated Universal Time**
- Registered Mobile Number

Expanded Subscriber Content (sometimes referred to as Neoprint) will be delivered in PDF format and may include:

- Profile Contact Information
- Mini-Feed
- Status Update History
- Shares
- Notes
- Wall Postings
- Friend Listing, with Friends Facebook ID's
- Groups Listing, with Facebook Group ID's
- Future and Past Events
- Video Listing, with filename

Courtesy: EFF

Annexure VI
Activity: Case Study

Case Facts:

Ruchi, a student of class VIII accepted a Facebook friend request of Ranbir who was a senior in class XII and one of most popular kids in school. Over time, the two chatted and became close friends on Facebook. Ranbir asked Ruchi to be his girlfriend and requested intimate pictures of her over his email (Gmail). Ruchi agreed to do so and sent the pictures. Later she regretted her decision. The next time Ranbir asked for the pictures, Ruchi denied. Ranbir threatened Ruchi saying if she does not send her pictures, he will spread her naked pictures and also show these to her parents. The next day the entire school had received these photos over their WhatsApp. Ruchi approached the cyber cell.

Statutes and Provision for the Chargesheet:

Information Technology Act

POCSO

IPC

Investigation

Glossary

Cyber Stalking: Act of repeatedly or constantly following or contacting a child through social media or any internet services. Acts like sending multiple friend requests and unnecessary tagging in pictures may amount to cyber stalking.

Deep Web: It is that part of the Internet or the world wide web which you cannot access via conventional internet browsers like Google Chrome, Internet Explorer, Firefox etc. Also referred to as the darknet, it is that part of the internet which runs in closed networks generally used for anonymous communication and commission of illegal activities.

Electronic Evidence: Any documentary evidence in an electronic form whether or not original.

I.P. Address: Stands for Internet Protocol address. It is a string of numbers (for example 112.79.141.75) which identifies one or more devices on a network. One can compare it with a postal address of a device on the internet with the only difference being that IP addresses are dynamic, meaning that they keep changing from time to time. Additionally, an IP address can be public and private. Public IP address can be accessed over the Internet globally. Private IP address is used to assign addresses to devices within a private space or network.

Online Enticement: Attracting or luring a child to do an act in lieu of something. Often done through offering children gifts on online games.

Online Grooming: Use of social media or other internet based services to prepare or train a child for some particular activity. Usually done to take sexual advantage of children by gaining their trust through building relationships.

Trolling: The act of harassing someone in an online community (closed or public) by posting text, audio, video, images etc. about them or insulting them through direct messages.


CYBER PEACE FOUNDATION
unicef
for every child
Helpline
+91 957 0000 265
helpline@cyberpeace.net

To donate online, scan QR Code

unicef
for every child

www.cyberpeace.org

email: secretariat@cyberpeace.net

TOGETHER WE CREATE
A PEACEFUL CYBER SPACE

INDIA : +91 651 6458865 USA : +1 71624 11555 UK : +44 20 32870765

cyberpeacefoundation @cyberpeacefoundation @cyberpeacengo