Cyber crimes against Women & Children

Prof(Dr)Debarati Halder, LL.B, M.L., Ph.D(Law)(NLSIU, Bangalore)
Managing Director (Hon)
Centre for Cyber Victim Counselling
www.cybervictims.org
profdebarati@gmail.com
The core issue:
Why Women & Children?
## Typology of online crimes against women & Children

<table>
<thead>
<tr>
<th>Recognised by law</th>
<th>Indian Penal Code, Information Technology Act, Indecent representation of women prohibition Act, Protection of women from sexual harassment at workplace, POCSO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Voyeurism, cyber stalking, defamation, criminal intimidation, capturing sexual offence including rape, unauthorised access to device, data, denial of service attack, forcefully confiscating devices, creation of impersonating profiles, impersonation by misrepresentation, impersonation for cheating, violation of privacy, creation/distribution, production etc of sexually explicit contents, obscene contents, attempt to commit an offence, abetment to commit an offence, disclosure of information breaching a lawful contract even by intermediary (S.72A)</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulable behavioural traits especially with sexually explicit contents</th>
<th>Showing porn to children, making porn contents by using children,</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Non regulable offences &amp; behaviours</th>
<th>Revenge porn, Bullying, trolling, doxing,</th>
</tr>
</thead>
</table>

DrDebaratiHalder
Why you need to understand nature & terminology of such offences?

- Punishments may be different
- Service providers/intermediary may have different policies
- Legal understandings may be jeopardised.
Conceptualising privacy

- No one should disturb when one wants privacy.

- No one should be allowed to enter the premises / room / snoop into digital devices without any solid reason.

- No one should be unnecessarily questioned about the work / activity done when in private mode.
Representation of information, knowledge, facts etc. & includes different kinds of data

Processing of the said data can be done in the computer, computer system etc.

Data

Can be in any form recognized by computer, computer system etc.

Data can be personal, public or governable.
Processing needs to be done consensually.
The Personal Data Protection Bill, 2018

Data

- Biometric data
- Anonymized data
- Sensitive personal Data
- Genetic data
- Financial data
- Health Data
- Personal data
Who are the data generators? Processors? Data storing bodies?
Is it only the social media?

Chosen platforms

<table>
<thead>
<tr>
<th>FB, Instagram</th>
<th>WhatsApp, SnapChat</th>
<th>TikTok, YouTube</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace data bank</td>
<td>Hospitals, schools, colleges data bank</td>
<td>Service providers data bank</td>
</tr>
</tbody>
</table>
Are we creating ethical & legal data?

- Sharing information on WhatsApp groups
- Facebook posts
- Instagram posts and groups
- Virtual classes
Types of subject matters that may attract privacy

- Sensitive personal data
- Information privacy
- Data privacy
- Physical privacy
- Digital privacy
Do we have legal rights to protect our privacy

- Physical privacy flowing from UN Convention of Human Rights
- Art 21 of the Constitution of India
- Indian Penal Code
- Information Technology Act, 2000 (amended in 2008) & some of its Rules
- Juvenile Justice Care and protection of Children Amendment Act, 2015
- Protection of Children from sexual offences Act
- Data Protection Bill, 2018

- European Union General Data Protection Regulations
- Domestic data protection related laws in different countries
- 4th Amendment to the constitution of the US providing rights against unreasonable search, seizure etc.
Can our data be protected?

- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. (S.43A IT Act, 2000, amended in 2008)

- Disclosure of information breaching a lawful contract even by intermediary (S.72A)

- Exceptions to S.79, IT Act: Due Diligence not applied
Cyber penology

Procedural understanding
The common question: Which offences are cognizable, who can investigate

- S.77B IT Act: Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

- 78 Power to investigate offences. - Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector shall investigate any offence under this Act.

DrDebaratiHalder
Why police/websites may not show interest in cases of cross jurisdictional crimes

- Where it was *committed*
- Where the *effect* was felt
- Offender belongs to *which country*
- *Whether the website is a passive website, interactive website or mixed website*
How would one understand that data has been breached

- Suspicious mail /message /contents
- Change of profile contents
- Impersonating profiles/mails reaching out to contacts
- Outflow of banking data/ money
- Receiving calls from suspicious persons
How to save your phone, data and contents

• School’s responsibility
• Liability of websites
• Filing complaint to the nearest police station
• Reaching out to SP /Judicial magistrate
• Two step verification system
• WhatsApp admin liability
• Cautious and judicious use of cloud storage
• Controlling self generated data
Best practices vs worst practices

- Protect the evidence
- Contact the website/company hosting personal data
- Contact the police on an urgent basis
- Reboot the devices
- Refresh all passwords/user ids.

- Do not contact hackers
- Do not reach out to senders of suspicious mails/messages
- Do not destroy the evidences
- Do not go ahead with old passwords, user ids.
Search & Seizure by the police and how to help them

<table>
<thead>
<tr>
<th>Hardware</th>
<th>other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Last seen page, screen shots etc,</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Websites visited</td>
</tr>
<tr>
<td>Memory chip/drive/card</td>
<td>Digital footprints of the victim</td>
</tr>
<tr>
<td>Hardware contents</td>
<td>Time stamps on messages,</td>
</tr>
<tr>
<td>Server infrastructure</td>
<td>mails, photographs, bank</td>
</tr>
<tr>
<td>Router</td>
<td>transactions etc, header of the mail</td>
</tr>
<tr>
<td>Any other chip included/</td>
<td>URL, phone numbers, call &amp; message</td>
</tr>
<tr>
<td>attached ATM machines used</td>
<td>log, Payment gates used, Bank server, SMSs.</td>
</tr>
</tbody>
</table>

DrDebaratiHalder
What to do with the offender?
How to handle the victim?

Reformative punishment
Repairing the damage
Restricting internet & device usage
Removing all sensitive data from the device & cloud storage
No contact order (Halder, 2016, 2018)

- Counselling
- No victim blaming
- Reintegration with the social network
- Compensation
- Preventing from taking up Irrational Coping mechanism (Halder, 2014)
Thank you
Prof(Dr)Debarati Halder
Managing Director (Hon)
Centre for Cyber Victim Counselling
www.cybervictims.org
profdebarati@gmail.com
For more information on Cyber law please visit
Gender and Internet : web magazine for cyber law for women
@ https://internetlegalstudies.com/