Characteristics of Cyber Sextortion in India: Content Analysis of Online Newspapers Published in 2019–2021

Himel Mondal1, Manas Ranjan Sahoo2 and Shaikat Mondal3

Abstract

Introduction: Smartphones and Internet connection help people to stay connected to virtual social media where predators may disguise and obtain intimate text, audio, photographs, and video from the victim. These are then used to extort money, sexual act, or any other favors.

Aim: We aimed to observe the characteristics of cyber sextortion in India in recent years (2019–2021).

Methods: This was a cross-sectional observational study conducted in February 2022. The cases of cyber sextortion reported in newspapers between 2019 and 2021 were considered for qualitative analysis. The cases were thematically analyzed by 2 authors individually and a consensus was reached for the finalization of the finding.

Results: Social media and dating applications are used to lure the victims to exchange sexual text, intimate photo, or video. The contents are saved and used as a tool to extort money, sexual acts, or other favors. The males are commonly extorted for money but females are extorted for money and sexual acts. The victim may be called for a sexual act in a place and a group of extortionists may appear in the scene. Exchange of text messages or audio calls are also recorded for extortion. Personal intimate contents obtained from remote access of device or access through a third person or morphing videos are also used for sextortion.

Conclusion: Social media engagement and a desire of exploring sexual relations with unknown persons expose the victims for sextortion. Storing and sharing intimate content should be avoided even when in trusted relations to minimize the risk.

Keywords
Social media, smartphone, text messaging, sextortion, India

Introduction

“Sextortion” is the practice of extorting money, sex, or other favors by threatening the victims to share their intimate photo, audio, text, video, or other media on the Internet or with closed social groups.1 There are several definitions of sextortion available on online dictionaries. Some of them are listed in Table 1. From the definition, it is evident that the extortionists pressure the victim to have sex with the extortionist (or others) or take money. However, the extortionist may also start blackmailing the victim to get other forms of advantages like an advantage in a job posting, selection in an interview, photos or contact number of others, fixing a date with others, and so on.2 Although the term sextortion is not a new one, its usage of the terms as found in

1 Department of Physiology, Saheed Laxman Nayak Medical College and Hospital, Koraput, Odisha, India
2 Department of Psychiatry, Fakir Mohan Medical College and Hospital, Balasore, Odisha, India
3 Department of Physiology, Raiganj Government Medical College and Hospital, Raiganj, West Bengal, India

Corresponding author: Himel Mondal, Department of Physiology, Saheed Laxman Nayak Medical College and Hospital, Koraput, Odisha, India.
E-mail: himelmkcg@gmail.com
The reason for this rise may be attributed to either higher incidents of the cases of sextortion or a higher rate of publication of the cases. However, it is difficult to actually gauge the reason for the higher increase. In addition, it is difficult to estimate the prevalence of sextortion in society as the cases coming into the limelight may be actually the tip of an iceberg. In India, many of the cases may be suppressed by or negotiated between the victim and the extortionist. Only the cases where the victim finds difficulty in handling the matter seeks help from the law enforcement system. However, mental and physical torture or monetary loss is there in each and every case of sextortion.

From the definition of sextortion, it is perceivable that it is not a new type of crime. The earliest case in India was reported in 2006. However, with the recent popularization of smartphones, cheap Internet connection, access to pornography, and increased use of social media, the form of sextortion is frequently associated with online communication. Hence, we are using the term “cyber sextortion” by combining the “cyber (meaning ‘relating to or characteristic of the culture of computers, information technology, and virtual reality’)” and “sextortion” in this article. A recent report from Thane (a metropolitan city in Maharashtra, India) cyber police states that approximately 42% (25 out of 60) of the registered cases in the station are about cyber sextortion. During the COVID-19 pandemic, the cases had increased almost double than the cases reported before the lockdown.

In this study, we qualitatively analyzed the content of cases of cyber sextortion in India that are published in online news portals. The finding would help us to appraise the society, psychiatrists, or psychologists dealing with the cases related to sextortion, and stakeholders involved in law enforcement to prevent the cases of sextortion in the country.

Google Ngram Viewer (it shows the frequency of a word used in printed media) shows a sharp rise in recent years (Figure 1).

The usage pattern of the word “sextortion” and “Sextortion” as found in Google Ngram Viewer from 2000 to 2019 is shown in Figure 1. The definition of “Sextortion” in online dictionaries is provided in Table 1.

Table 1. Definition of “Sextortion” in Online Dictionary

| Dictionary | Definition of “Sextortion” | Threatens to Get From the Victim | Source Website |
|------------|---------------------------|---------------------------------|---------------|
| Cambridge  | “The practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them.” | Sexual act; anything else | https://dictionary.cambridge.org/dictionary/english/sextortion |
| Collins    | “If someone is subjected to sextortion, they are forced to do something, especially to perform a sexual act, by someone who threatens them with violence or to expose their sexual history.” | Sexual act; anything else | https://www.collinsdictionary.com/dictionary/english/sextortion |
| Oxford     | “The practice of extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity.” | Money; sexual act | https://www.lexico.com/definition/sextortion |
| MacMillan  | “The crime of trying to get money from people by persuading them to perform sexual acts that are filmed on a webcam and then threatening to share the film with friends, family, employers, etc.” | Money | https://www.macmillandictionary.com/dictionary/british/sextortion |

Source: Online dictionary websites; available on the right most column of the table.
Methods

Ethics
This study involves an audit of qualitative data available on public domain websites. No identification data of extortionist or victim was used in this manuscript. However, anonymous example cases are presented in this article. This study does not require any clearance from Institutional Ethics Committee.

Type and Settings
This was an observational, retrospective, qualitative study where we analyzed the contents of cases of sextortion published on online news portals in 2019 to 2021 periods. For the study, we only included the newspapers available online on public domains. For the data collection, we used a personal Windows computer with a cookie-cleared browser—Mozilla Firefox (version 97.0). The data were collected between February 5 and February 20, 2022 by the first author.

Search Strategy
We searched the news with defined keywords from various Internet sources. The keywords were as follows: “sextortion,” “cyber sextortion,” “sexual exploitation,” and “online sexual extortion.” We searched the keywords in Google news (https://news.google.com/), Google (https://www.google.co.in/), Yahoo News (http://news.yahoo.com/), and Bing (https://www.bing.com/). These websites help searching the news articles published online. The news published in the Indian news medium about sextortion cases of India was only saved for analysis. During data collection, we removed the duplicate entries by comparing the date of publication, place of incident, characteristics of the victim or extortionist, and details of the incident. The data collection was continued till the thematic data saturation.

Data Analysis
The cases were analyzed to extract the nature of the sextortion cases by 2 authors individually and a consensus was reached for the final qualitative result output. The data were collected till the thematic data saturation. Example of anonymous cases for each theme was presented in the result. There are many cases where there may be overlapping of some of the themes from other cases.

Results
We thematically analyzed the textual content of 36 cases of cyber sextortion that occurred in different states of India. Theme-wise finding is presented below.

Male Versus Female in Money Versus Sexual Act
There is a different pattern of extortion according to the gender of the victim. If the victim is male, the extortionists commonly demand money in exchange for suppression of the content. If the victim is female, extortionists demand primarily sexual acts from the victim. However, they may extort money or some other favors in some cases.

Example 1
A middle-aged man was contacted via social media and he was engaged with explicit message sharing. Later, the extortionist started threatening to reveal the content and demanded money to suppress the matter.

Example 2
A female was engaged in a sexual relationship and later when she did not want to continue the relationship, the man started threatening to make their intimate videos online if she fails to continue the sexual relation.

Friendship in Social Media
Due to the higher use of the smartphone, the Internet, and social media, people are exposed to a virtual society. In this virtual medium, any predator can pose as a beautiful girl or handsome boy to lure the victim. A social media account with an attractive photo is used to make a first impression. The predator then starts exchanging messages or sharing some fabricated personal life story or problems he/she is facing in his/her personal or marital issue to induce empathy. Sometimes, the financial crisis is also expressed. When the predator can sense that the victim is optimally connected with the string, the next phase of action is started.

Example 3
A man was befriended with a woman in social media and exchanged the phone number and the woman made a video call and was shown explicit contents. The extortionist then demanded money in exchange of not releasing the video call record.

Example 4
A woman contacted a man on social media. The man was promised sexual relationship and when he went to the site, other people came and captured photograph and all of them started blackmailing with the photos.

Sexting Screenshot
After getting connected from social media, the victim starts exchanging sexuality related text with the virtual or fake
person. The meaning of the word “sexting” is “the action or practice of sending sexually explicit photographs or messages via mobile phone.” Message exchange in social media messenger is then saved as screenshots for evidence. Then the extortionist starts blackmailing with a threat to expose the chat history with spouses or friends or relatives.

**Example 5**

A man was engaged in exchange of sexual message with one girl he befriended on social media. After some days, a man started calling with demand of money to suppress the screenshot of messages.

**Prompted Video**

Connected with any social media messenger (eg, Facebook Messenger) or applications like WhatsApp, the predator shows prerecorded video content that seems live to the victim. For example, the victim can see a naked person masturbating on the screen. Then the victim is asked to start a similar act. When the victim starts doing the act, the screen is recorded and the blackmailing with the recorded screen starts. In addition, to live chat, the recorded video is also requested from the predator. First, the predator sends some recorded video and asks the victim to record a similar video and send it as a reply. By both the way of prompted sexual act-related video, the predators get access to the video that they use to extort money.

**Example 6**

A man shares some of his personal photos and videos as he got similar ones from his intimate friend. Then his friend started extorting money with a threat to reveal the contents to his family and friends.

**Video Call Record**

Here the victim receives a video call request from the extortionist. The caller may be known to the victim from social media or any dating app. However, the predator may call a random number and anyone receiving the video call request from the unknown number may be a potential victim. In this method, the extortionist makes a video call and when the receiver receives it, the extortionist plays or acts any sexual activity and the screen is recorded, and immediately after the call, threats come from the extortionist.

**Example 7**

A man was allured in a sexual video chat and the man started exposing him as he was shown a video where a woman was showing body parts. The video chat was recorded and was used as a tool of extortion.

**Example 8**

A man receives a video call from an unknown caller in a social media calling app. When the video call was received, sexually explicit content was played and the extortionist recorded the screen and started calling the victim for money.

**Promise of Sexual Engagement**

Victims are first targeted and a friendship is built with them. Then the victim is lured into a sexual act and is called into an area, either a lonely place or in a residential place. The victim, assuming a consensual intimacy, comes to the site. However, at the initiation of the intimacy, fake police officers or other persons enter and start threatening. They may capture the photo for keeping a piece of evidence. However, here the events are organized in such a way that the sexual act does not happen.

**Example 9**

A woman made friendship with a declared widow. The man was invited for a sexual relationship. However, before the sexual act, some people posing as police officers captured the man and demanded money to settle the matter at the site.

**Recording of Intimate Photos or Video**

This pattern of sextortion involves inviting the victim for a sexual act and the incidents are either captured as still images or video is recorded. The victims may be acquired from social media or personal contact. Either the predator or any partner captures the media that are later used to extort money. In addition, this happens between 2 persons in an apparently good relationship at the point of time when the videos were captured. Later, due to any reason, the predator may threaten to publish those explicit sexual contents on social media or send them to family and friends to extort further sexual acts, money, or any other favor.

**Example 10**

A boy found intimate photos of a girl that she captured with her boyfriend. They boy started extorting the girl for more naked photos and phone numbers of other girls with a threat to release the photos on social media.

**Example 11**

A girl who was in a relationship with a boy and captured their intimate photos and video. But when the girl wanted a separation, the boy started threatening the girl to continue the relation with a threat to reveal the personal photos and videos.
Audio Call Record

In this form, an audio call may come from an unknown number and a recorded audio (i.e., machine voice) may come with an assurance of fulfilment of any demand. Or the caller may pose that the call was mistakenly made to the victims’ number. When the victim reverts to call that number, a friendship is built, and later both engage in exchanging sexual talk. The predator records those calls and later starts extorting money from the victim.

Example 12

A call from an unknown number was received by a man. There was a woman on the other side. Both became friends, and gradually they were engaged in sexual talk. Later, the man was demanded money for keeping the recorded audio call secret.

Morphed Video Threat

With the advent of technology, many people are now sharing their photos and video content. Extortionists may fabricate some pornographic photo and video from the content and ask the victim or their parents to give money or the contents would be shared on social media. In addition, the extortionist may make his/her number identified as a police officer and ask the victim that the content came to him/her. Money is demanded suppressing the facts. The extortionist can also set a photograph of a police officer in his/her social media profile connected with the mobile number. Furthermore, with the help of Truecaller (a smartphone application for identification of unknown numbers where the callers’ name appears on screen from stored information on company servers), the extortionist may set a photo and name so that receiver gets the image and name of a police officer.

Example 13

A woman received a call from an unknown number and on receiving the call, an objectionable video was played. When she disconnected the call, a morphed video with the women’s face was shared with a threat to release on social media and demanded money to delete the video.

Intimate Photos From Other Sources

Photographs of intimacy may be accessed by hackers or close contacts either from direct access to electronic gadgets or installing some remote access application. These photos or videos may be used to blackmail the victim for money, sex, and other favors like more intimate photos, videos, fixing a date with others, and so on. This is not uncommon when a friend or lover becomes rogue and starts blackmailing with the media captured when the relationship was running smooth.

Example 14

A girl’s mobile was accessed by some boys and her intimate photos were stolen from the device. Later, they shared the photos in a closed group and threatened to have sexual relation to suppress the further spread of the photos.

The risk factors according to finding of this study are presented in Table 2.

Discussion

The incidence of sextortion has increased in recent years with the advancement of technology. Along with adults, adolescents are also found to be either victims or extortionists. A recent survey by Patchin and Hinduja found that nearly 5% of school students are under some sort of sextortion.11 To the best of our knowledge, there is no similar survey from India. In the

| Table 2. Risk Factors of Exposure to Sextortion |
|-----------------------------------------------|
| In Internet                                   |
| Using dating applications                     |
| Accepting unknown friends on social media    |
| Accepting unknown video calls                |
| Sexting on social media messenger            |
| Sharing sensitive personal photos or videos  |
| Posting personal matter (eg, disturbed relationship with spouse) in social media |
| In personal device                            |
| Talking too intimately with unknown          |
| Talking too intimately with lover            |
| Exchanging text message that are too personal |
| Capturing and storing too personal photos or videos |
| Installing unknown or prompted applications in smartphone or computer |
| In a relation (friendship, love, or marital) |
| Capturing photographs or video of sexual acts and storing it |
| Showing personal photos to friends           |
| Showing personal photos of others (that was obtained from any avenue) to friends |
| In profession                                |
| Obtaining or providing something with exchange of sexual acts |
majority of the reported cases, the victims are commonly adults. However, there may be many underlying cases in school-going adolescents that remain unreported. The underlying reason may be the social obligations of India. However, parents, teachers, and family members should handle the case with full mental support to the victim.12

It is to remember that the extortionists may not stop blackmailing the victim even after payment of money or involving in sexual relations, or any other forms like sending additional photos or videos. Hence, the case may be immediately reported to the cyber police. Recently, the reporting of cybercrimes has been increased and a significant percentage is of sextortion. With this reporting, perhaps the extortions are being traced and further actions are being taken by the prevailing law.

Access to social media has increased due to higher smartphone penetration during the COVID-19 pandemic. The school and college-going students were having no option but to attend online classes from smartphones or other devices from home. In addition, the evaluations were also made in online mode.13 The lockdown created a situation where recreation became online too. Hence, adults and adolescents might be finding a virtual friend and eventually fell into trap of sextortion. The reported case along with online search trends of the term “sextortion” was increased with the initiation of the lockdown as shown in Figure 2.14

The extortionist commonly uses social media to target the victims. Even if the social media profile is locked for unknown visitors, the extortionists may make friends with a common friend and then with the victim. Hence, whenever an extraordinary behavior is seen in some of the online friends who are unknown in real life, it should be flagged as a potential cause of harm. Further attachment should be avoided. However, in some cases, some personal moments are captured in a romantic relationship. Then, due to the disturbance of the relationship, one of them becomes a victim, and another becomes extortionist. Hence, capturing and storing personal moments should be avoided.

A recent trend is video calls from an unknown number. When the receiver connects the video call, objectionable content is shown, and with the screen-recorded video, extortionists start blackmailing. Hence, calls from unknown numbers should be avoided. Sometimes morphed videos or photos are edited to place someone’s face on explicit sexual content. Whatever may be the form of extortion, the victim always fears their social image to tamper. Hence, family, friends, and society should take positive and constructive steps to prevent such mental trauma. A victim should not be further traumatized. Awareness about safe digital behavior needs to be promoted in schools and colleges as well as television, radio, or printed media.15,16

Due to lockdown, many of the doctors started telemedicine services via video calls. In a bizarre event, a doctor received a call and thought the call was from a patient. However, the caller showed explicitly sexual content, recorded screen video of the call and started threatening to release the video, and demanded money. Hence, doctors should be careful before starting a video consultation, and preconsultation methods like taking an audio call first to get basic information, demographics, consent for telemedicine, and consultation fees before video consultation should be followed to avoid such events.17 If it happens even after the precautions, the case should immediately be taken to the cybercrime police.

The cases of cyber sextortion can be registered in the Indian National Cyber Crime Reporting Portal (https://cybercrime.gov.in/).

![Figure 2. Worldwide and Indian Internet Search Trends for the Term “Sextortion” in Five-Year Period (April 2019-December 2021) as Found in Google Trends](https://trends.google.com/trends)
Limitation
The study is based on the cases published in newspapers. However, we adopted this method as surveying this sensitive issue was difficult with our limited resources. With a glimpse of the case, it was not possible to find victims’ details demographics. Hence, it was not presented.

Conclusion
Unsafe social media behavior and a desire to be engaged in romantic or sexual relations with unknown persons expose the victims for sextortion. Hence, social media should be used with utmost privacy, and the exchange of too personal facts, images, and videos should be avoided. Texting, talking, or video calling with unknown and befriended in social media should be minimized to avoid the risk of sextortion. Capturing and storing intimate content in devices should be either avoided or the devices should be protected so that the contents are not accessed by anyone else. Awareness programs should be promoted to appraise the society about the risks of sextortions so that they can avoid those risks.

Author Contributions
HM: Concept, design, literature search, data analysis, and drafting manuscript; MRS: Data analysis, literature search, and editing manuscript; SM: Concept, graphics, and editing manuscript.

Declaration of Conflicting Interests
The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

ORCID iD
Himel Mondal https://orcid.org/0000-0001-6950-5857

References
1. O’Malley RL, Holt KM. Cyber sextortion: an exploratory analysis of different perpetrators engaging in a similar crime. J Interpers Violence. 2022;37(1–2):258–283.
2. Wolak J, Finkelhor D, Walsh W, Treitman L. Sextortion of minors: characteristics and dynamics. J Adolesc Health. 2018;62(1):72–79.
3. Google Ngram Viewer. Sextortion. https://books.google.com/ngrams/graph?content=sextortion&year_start=2000&year_end=2019&corpus=26&smoothing=3&caseInsensitive=true. Accessed on February 20, 2022.
4. Chand S. Sextortion cases on rise, be careful on social media. The Times of India. https://timesofindia.indiatimes.com/city/delhi/cases-on-rise-be-careful-on-social-media/articleshow/89463312.cms. Accessed on February 20, 2022.
5. Hong S, Lu N, Wu D, Jimenez DE, Milanaik RL. Digital sextortion: internet predators and pediatric interventions. Curr Opin Pediatr. 2020;32(1):192–197.
6. Yadav Y. India becoming ‘sextortion’ capital of the world? The Times of India. https://timesofindia.indiatimes.com/blogs/voices/india-becoming-sextortion-capital-of-the-world/. Accessed on March 26, 2022.
7. Vinnakota D, Arafat SMY, Kar SK, et al. Pornography and sexual violence against women in India: a scoping review. J Psychosex Health. 2021;3(3):216–221.
8. Gharat A, Mengle GS. Cases of sextortion – extortion through sexual methods – on the rise in Thane. Hindustan Times. https://www.hindustantimes.com/cities/mumbai-news/cases-of-sextortion-extortion-through-sexual-methods-on-the-rise-in-thane-101636724264387.html. Accessed on February 20, 2022.
9. Arafat SMY, Menon V, Vinnakota D, Saroj A, Kar SK, Kabir R. Studies on sexual behavior during COVID-19 pandemic: a bibliometric analysis. J Psychosex Health. 2022;4(1):20–25.
10. PTI. ‘Tip of the iceberg’: sextortion, hacking abound as cybercrime against women increases amid lockdown. News18. https://www.news18.com/news/india/tip-of-the-iceberg-sextortion-hacking-abound-as-cybercrime-against-women-increases-amid-lockdown-2601039.html. Accessed on February 20, 2022.
11. Patchin JW, Hinduja S. Sextortion among adolescents: results from a national survey of U.S. youth. Sex Abuse. 2020;32(1):30–54.
12. Gassó AM, Klettke B, Agustina JR, Montiel I. Sexting, mental health, and victimization among adolescents: a literature review. Int J Environ Res Public Health. 2019;16(13):2364.
13. Mondal H, Sahoo MR, Samantaray R, Mondal S. Medical students’ perception on the usefulness of online formative assessment: a single-center, mixed-method, pilot study. J Edu Health Promot. 2021;10:243.
14. Press Trust of India. “Significant” increase in cyber crimes against women during lockdown: experts. NDTV. https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352. Accessed on February 20, 2022.
15. Mori C, Temple JR, Browne D, Madigan S. Association of sexting with sexual behaviors and mental health among adolescents: a systematic review and meta-analysis. JAMA Pediatr. 2019;173(8):770–779.
16. In Focus. Meet Anuraag Singh cyber expert who is educating young people about cyber sextortion. Deccan Chronicle. https://www.deccanchronicle.com/in-focus/180222/meet-anuraag-singh-cyber-expert-who-is-educating-young-people-about-cy.html [Last accessed on 20 February 2022].
17. Mondal H, Mondal S. Brief technical guide for teleconsultation. Indian Dermatol Online J. 2020;11:812–815.