Indian Journal of Health, Sexuality & Culture
Volume (6), Issue (1), June 2020
ISSN 2581-575X
https://www.iisb.org./

Review Article

Online sextortion

Saloni Agrawal
National Law Institute University, Bhopal, Madhya Pradesh, India

Date of Submission :
2 April 2020
Date of Acceptance :
3 May 2020

Abstract
Online sextortion is a pervasive cybercrime. In this, perpetrator tends to harass victims by invading their privacy and threatening to release and disseminate the victim's intimate images in public if they didn't comply with the demand of additional sexual favors or money. Online sextortion has an acute impact on the mind of victims. It is necessary to support and encourage victims in their fight. The present article aims to provide a comprehensive understanding of online sextortion and the preventive measures that can be taken to stop this cybercrime. There is a need for robust legal frameworks to minimize this cybercrime.

Keywards: Sextortion, Online sextortion, Sexual extortion, Cybercrime

Introduction

The digital era has brought in with it the advancement of technology for the use of mankind. Technology has helped humans to achieve great heights. Now, information is just a click away. Anyone from anywhere can easily access the internet to get information and upload information. The internet has become part and parcel of human life. The young generation can be seen using personal computers, laptops, mobile phones, digital cameras, iPods, etc.

Though the internet has its good side and various advantages, it has been used by various people for criminal activities which are commonly known as cybercrimes (Maharashtra Cyber, Home Department, 2020). Cybercrime, as defined by National Cybercrime Reporting Portal, is *"any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime"* (Indian Cybercrime Reporting Portal, n.d.). Cybercrimes include child pornography, sexting, cyberstalking, online sextortion, etc.

Today, social media is used by everyone in every part of the world. Anyone can become a friend of another without even seeing the person in real life. People have started dating online and have termed it as 'online dating'. While some of these online relationships have become successful, many have fallen into the trap of fake accounts. According to a 2015 United Nations report, up to 40% of young people aged below 18 years self-

Corresponding Author : Miss Saloni Agrawal
E Mail: saloniagarwal.ug@nliu.ac.in
How to cite the article : Agrawal, S. (2020). Online sextortion. Indian Journal of Health, Sexuality & Culture, 6(1), 14-21.
DOI : 10.5281/zenodo.3929135

generated and shared sexually explicit content online (United Nations Office on Drugs and Crime, 2015). Many of the social media accounts are easily hacked and personal information is used to blackmail and threaten such victims (Goldstein, Tov, & Council., 2018). One such cybercrime is online sextortion wherein perpetrators of such fake accounts or the hackers tend to get intimate and private images of the victim and threaten to release these images if they did not comply with their demands.

This article explains the meaning of online sextortion, makes the readers aware of cases of sextortion that happened around the world. This article also brings to the notice of the stakeholders that there lacks research on psychiatric disorders among perpetrators of online sextortion. The article attempts to highlight the social and psychological impacts on the victim by sextortion. The second part deals with the steps that victims may take when they are being sextorted and the preventive measures to avoid sextortion. In the third part, the author attempts to emphasize the need for the active awareness of the people and the need for the well-framed law on sextortion.

Online sextortion

Online sextortion is a type of extortion in which a person threatens to release or distribute private sexual and intimate images, videos, or any such material of victim if the victim doesn't engage in further sexual activities or does not provide money to the perpetrator (E-Safety Commissioner, n.d.). Online sextortion is a form of sexual harassment, exploitation, coercion, and violence. It is terrifying and de-humanizing. The phenomenon of online sextortion is worldwide. It is more prevalent in countries like U.S.A., Canada, Philippines, U.K., China, Japan, etc.

Online sextortion is a very serious issue. It can take place from anywhere by anyone in the world. It affects the victims emotionally, mentally, and sexually. Online sextortion may vary. Most of these cases involve (Thorn, 2017)

- **Manipulating victims through social media:** Perpetrator mostly gets close to the victims with the help of social media. Perpetrator chats on these social networking apps and creates a type of environment for the victim that he/she fully trusts the perpetrator. Many victims get tricked in online relationships with these perpetrators. Victims send them their private images or videos. Perpetrators then threaten the victims for sexual favors as demanded or money for not leaking the images or videos.
- **Hacking**: Perpetrator may intrude into the social media account or email account or hack the device such as laptops, computers, or mobile phones, etc. wherein the victim has stored his/her private sexual or intimate images and thereby get access to these files to harass and threaten the victim.

There are instances where the perpetrator had threatened to distribute, reveal, or disseminate photos. In the case of United States v. Beckett (the United States v. Beckett, 2010) and State v Stancl (State v. Stancl, 2009), perpetrator pretended to be a teenage girl on social networking sites and tricked schoolboys to send their nude photos. Once the perpetrator had these photos, he threatened to disseminate the photos if they didn't engage in sex or didn't fulfill other sexual demands made by him.

There are instances where the perpetrator had not only threatened but also has disseminated the images and videos. In United States v. Hutchinson (the United States v. Hutchinson, 2014), the perpetrator had created a fake account on social media. He deceived the girls, obtained nude photos, and contact information of them. He

threatened to reveal these photos to the family and friends of the victims if they didn't provide him with more sexual images. He has also released and posted photos online of those who didn't act under his demand.

Online sextortion is prevalent in many cities in India as well. There are cases such as the infamous case of the Punjab and Haryana HC where a girl was blackmailed by three seniors of her university to release her nude images in public. She was also raped by them (Nayar, 2015). Another story is a case of Mumbai where a classmate of a girl maliciously hacked the account of her boyfriend and had access to the nude photos of the girl which she sent to her boyfriend. He wanted and liked the girl and threatened the couple to post the nude photo of the girl in public (Mihindukulasuriya, 2019). There are other cases of Mumbai wherein Cyber Police says that the victims have complained that they have visited a certain pornographic website and thereafter received an email stating their full names and all the contents they have watched along with a message demanding money in the form of cryptocurrency. The message also added that if they didn't comply with the demand, the said pornographic details will be released on the victim's social networking accounts which were also hacked by the perpetrator (Mengle Enter, 2018).

Online sextortion can be done with many victims by a single perpetrator. It can be seen by this case where thousands of underage girls were targeted by a guy. He either hacked their accounts or their devices to obtain their obscene images. He sent emails to girls threatening them to release these images in public or harm their family members if girls didn't send more images of their bare breast and vagina, didn't finger in front of a webcam, or didn't fulfill any such demands made by him.

A survey was conducted by Microsoft in 2017 across 14 countries through Digital Civility Index. Findings indicated that 77% of Indians have reported concerns about sextortion, revenge porn, or unwanted sexual solicitation (Microsoft News Center India, 2017).

Online sextortion takes place with many in India and around the world. This has affected children, adults, vulnerable groups, and established professionals. Not only women but also men, gay, transgender, and gender non-conforming people are affected. Few people report cases of online sextortion because they feel ashamed and degraded and they couldn't bring the case to the concerned authorities (Thorn, 2017).

An insight into mind of perpetrators

The basic question always arises that why a person commits a crime. There can be various reasons ranging from greed, anger, revenge, pride, jealousy to fun, and more. It depends on the type of crime committed (SCCJR, 2016). Online sextortion is a cybercrime which is one of the ways to sexually assault and exploit the victims by threatening them. Some researchers have covered the question as to why perpetrators commit sexual harassment, sexual assault, rape of minors, rape of adult women, etc. But there is lack of research as to why perpetrators commit online sextortion.

Many factors play important role in the commission of this crime. First, it is committed to a digital world. Second, it involves either hacking into victims' device/ account or making victims trust the perpetrator to share their own sexually implicit images. Third, there is a threat involved which allows the perpetrator to extract favors from the victim. Fourth, favors can range from victims showing his/her intimate body parts to sexually hurting oneself for the pleasure of the perpetrator. These factors suggest that it is different from the cases of sexual harassment, sexual assault, etc and require in-depth research in the psychology of the perpetrator. By

considering the above four mentioned factors, it can be said that perpetrators do not commit this crime out of rage but it is well planned and executed.

Perpetrators can fall under any of these categories: minor-focused cyber sextortion perpetrators, intimately violent cyber sextortion perpetrators (O'Malley & Holt, 2020), perpetrators of sexual assault against adults and perpetrators who are minor (Robertiello & Karen, 2007) and accordingly the reasons for committing this crime can vary. As a general understanding, this crime can be committed for reasons such as revenge, fun, need for money, substance abuse, or due to personality disorder or psychiatric illness. Yes, there is a possibility that perpetrators may have committed online sextortion due to psychiatric illness and personality disorders. One such psychiatric disorder can be sadism as perpetrators derive their sexual pleasure from inflicting pain and humiliation on victims. There is a need for research in the possible personality disorders or psychiatric illness in perpetrators. Researchers must delve deep into the question and find relevant information as the crime of online sextortion have a great impact on the minds of the victim.

Social and psychological impact of online sextortion on victims

The impact of information & communication technology and the cyber world on society is undeniable. Online sextortion and its effects have a lasting impact on the mind of victims all over the world. The victims feel a loss of control. They go into a stage of grief and develop a sense of shame (Jurecic, Spera, Wittes, & Poplin, 2016).

Even today, sexual matters are not openly discussed in society. They are considered a sensitive subject (Motsomi, Makanjee, & Nyasulu., 2016, Turnball, 2012). In this scenario when perpetrators threaten victims to disseminate and release their private, sexual, and intimate images in public, then victims feel fear, betrayed, angry, anxious, embarrassed, and guilty (Orick; Herrington; LLP Sutcliffe; Legal Momentum, 2016). Victims who fulfill the demand of the sextortionists, are forced to perform sexual favors such as masturbation, strip dancing, drinking their ejaculation, fingering, fisting, anal fingering, spanking, etc. in front of webcam. Sexual activities are pleasurable but done under coercion or threat, it becomes sexual assault. The time spent under the control of the sextortionist is dreadful and horrendous. All this is real and the harm is irreparable (Jurecic, Spera, Wittes, & Poplin, 2016).

It is easy to blame the victims in cases of sextortion as they are the ones who have clicked their intimate images or videos or sent such materials to the sextortionist. The victims feel that the only option they have is isolating themselves from society (Leukfeldt & Malsch, 2018). Children who are the victim of this are affected the most. They are condemned by their family and friends. Young victims fear their social reputation and reputation of their family in the society. They fear of being terminated from their jobs and prospects. Victims succumbed to these thoughts and therefore fall and fail to come out and lodge complaints against such perpetrators. They always have fear of threats and the release of their private images and videos. This drains the victims emotionally. This also affects the victims mentally. Sextortion sexually harasses, exploits, and assaults the victim. All these lead victims to depression, overthinking, and self-isolation from the family and society. They either fulfill the demands of the perpetrator or commit suicide.

It is seen that victims generally have the feeling that no one can understand what their emotions are. They worry about what others will think about them. They generally say that they can't trust anyone again (Hinduja,

2016). Victims must realize that it is not their fault and they didn't deserve this. There are people like their spouse, family, friends, etc. who they can trust. Victims might be facing a lot of different emotions but at the end of the day victims must remain positive as taking one's life is not a solution. They have the right to be treated with respect and dignity. They have the right to get help and be safe.

Steps that should be taken by the victims

It is important to stay safe and secure in the cyber world. It is advised that victims should not fulfill the demand of the perpetrators as demands and threats keep on increasing and victims find themselves in a vicious circle.

Steps that should be taken if a person is being extorted: (Cybertip, n.d.)

- Victims should be calm and rational.
- They should immediately stop all the communication from the perpetrator.
- They should never send money or additional sexual favors as demanded to the offender.
- Victims should inform someone about the threat such as spouse or parents.
- They should keep all the information they have about the perpetrator such as their user names of social media accounts, any images or documents sent by the offender, email address, or any such thing. They shouldn't delete anything sent by the perpetrator.
- Victims should report everything immediately to the nearby police station or cyber crime department.
- Victims should report immediately if the photo or video is posted online to the online content host (Humelnicu, 2017).
- Victims should be made to consult a counselor.

Steps to prevent online sextortion

Seeing how dreadful online sextortion is for a person, one should keep certain things in mind to prevent themselves from getting sextorted. In this digital era, one must know how much privacy they have while using their personal devices such as mobile phones, laptops, computers, etc. One can stop his/her spouse or family members from using their devices. But without one's awareness, their devices can be tracked, their information and data can be acquired by a third party easily (Fosdick, 2019). Therefore, the individuals must be cautious and take extra care while using their devices to avoid such cybercrime. Some preventive measures to avoid online sextortion are as follows: (Humelnicu, 2017; Legal Momentum, n.d.)

- One must not store their intimate, sexual private images or videos in their devices as devices are connected to either one's email account or cloud.
- One must not share their sexual and private images or videos with any other person on social networking accounts as these accounts can get easily hacked.
- One must cover webcams when indulging in some sexual activity while using a computer or laptops.
- One must use anti-virus software in their device.
- Don't interact with the person you personally don't know on social media.
- One must be careful while changing their clothes in trial rooms or hotel rooms and restrooms.
- One must reduce and eliminate internet addiction.

Steps parents should take to prevent their child from being sextorted: (FBI Pittsburg, 2016)

- Parents must provide sexual and digital education to their children.

- Parents must be frank with and understand their children.
- Parents must monitor the online activities of their children.
- Parents must teach their children not to friend with or talk to anyone on social media they do not know in real life.

Steps educators and policymakers should take to prevent online sextortion:

- Parents and students must be made aware of the terrible cybercrime of online sextortion.
- Education must be provided on how to use and protect their social networking accounts from being hacked.
- Education must be imparted to everyone about the laws prevalent in the country pertaining to online sextortion.
- Cybercrime department should publish specific data and brochures on online sextortion.

Laws on online sextortion

At least 26 states in the USA have legislation on Sextortion (Greenberg, 2019). Federal state in the USA has also introduced 'the SHIELD Act' i.e. 'Stopping Harmful Image Exploitation and limiting Distribution Act, 2019' in the House of Senate to tackle the harmful issue of sextortion in the state. It proposes to criminalize knowingly distribution of intimate images, threatening to distribute the intimate images of a person in public. Offenders will be convicted for a term of up to 5 years and fine (Speier, 2019).

If the victim in India files a complaint of online sextortion then it will be treated under the Indian Penal Code, IT Act, or POCSO Act. No law in India defines or criminalizes online sextortion. Only the state of J&K in its Ranbir Penal Code (which is no more in existence) had included 'sextortion' as a crime under Sec 354E to prevent people from exploiting subordinates sexually (AK., A. 2020).

Indian Penal Code (IPC), 1860

- IPC, 1860 provides for the law of extortion under Sec 383 and Sec 384 which says that *"threat or fear used in order of delivery of material thing by the victim to the offender"* is punishable with the imprisonment for a term extending to three years or fine.
- *"Assault or use of criminal force to a woman with the intent to outrage her modesty"* is punishable with the conviction for 2 years term under Sec 354 of IPC.
- Sec 354C of IPC, 1860 says that if the perpetrator infringes the privacy of a person and disseminated his/ her private images then such perpetrator will be liable of conviction for a minimum period of 1 year which may extend to 3 years.
- Sec 292 of IPC, 1860 punishes the offender who sells or distributes obscene book, paper, or figure conviction for a term which may extend up to 5 years and fine.

IT Act, 2000

- Under Sec 66E of IT Act, a person can be convicted for the term of 3 years or fine up to 2 lakhs or both if he intentionally captures, transmits, or publishes the private image of a person in the public without his consent.
- Sec 67A of IT Act, 2000 punishes a person for the conviction for the term of 5 years and fine up to Rs. 10 lakh if that person publishes or transmits material which contains sexual implicit act electronically.
- Sec 67B of IT Act, 2000 punishes a person for the imprisonment of 5 years term if that person publishes or transmits material which contains sexual implicit act by children electronically.

POCSO Act, 2012

Under this act, a person who commits sexual harassment on a child is punished with the conviction for a term which may extend to 3 years. Sexual harassment includes making a child show or exhibits his body or a part of his body, threatening a child to release his real or fabricated sexually explicit images using electronic means.

It is recommended that policymakers make a separate law regarding online sextortion because present laws do not fulfill the elements of online sextortion. Online sextortion involves a threat to release sexual images of the victim. It damages and destroys the dignity of the victim. It forces victims to perform sexual favors for the perpetrator. It assaults victims sexually and mentally to the extent that sometimes victims take their own life. It should also be remembered that the crime of online sextortion can take place from anywhere by anyone in the world. The perpetrator can be from a different country and of a different nationality. It requires investigation to track the perpetrator. It is also recommended that law should be made strict and severe keeping in mind that once an image or video is uploaded, it is hard to be removed from all over the internet. It can resurface anytime. Repercussions that victim has to face are unimaginable and unfathomable.

Conclusion

Everyone can use the internet easily but few are aware of cybercrimes such as online sextortion. Online sextortion cases are increasing day by day. Many cases go unreported due to the mindset of the people. It is high time that the educators, policymakers, professionals make people aware of the increase in cybercrime and the remedies available to them. Researchers, psychologists, psychiatrists, and concerned stakeholders can analyze the reasons for the commission of online sextortion by perpetrators. It is also emphasized that the government should make well-defined laws regarding the issue of online sextortion in the country. At last, everyone must understand that 'your safety is in your hand' and it is important to be responsible for own actions in this technology-driven world.

References

AK., A. (2020). Sextortion, modifications to Arbitration Act, CrPC: The 37 Central laws that have been made applicable to J&K. Retrieved from https:// www. barand bench.com/news/ sextortion-modifications-to-arbitration-act-crpc-the-37-central-laws-that-have-been-made-applicable-to-jammu-kashmir

Cybertip Ca. (n.d.). Sextortion. Retrieved from https://www.cybertip.ca /app/en/ internet _ safety-sextortion.

E Safety Commissioner. (n.d.). Deal with Sextortion. Retrieved from https:// www. esafety.gov.au/key-issues/image-based-abuse/ take-action/deal-with-sextortion

FBI Pittsburg. (2016). Sextortion affecting thousands of U.S. children. Retrieved from https:// www.fbi. gov/ contact-us/field-offices/pittsburgh /news/ press-releases/ sextortion-affecting thousands-of-u.s.-children

Fosdick, H. (2019). Privacy in a Digital Age. Retrieved from http://uniforumchicago. org /slides/Meaning_of_Privacy.pdf.

Goldstein, D. K., Tov, D. O., & Council., M. D. (2018). The Right to Privacy in the Digital Age. Human Rights Council.

Greenberg, P. (2019). Fighting Revenge Porn and 'Sextortion'. Legis Brief .

Hinduja, S. (2016). Sextortion. Retrieved from https://cyberbullying. org/ sextortion

Humelnicu, I. V. (2017). Sextortion - The Newest Online Threat. AGORA International Journal of Administration Sciences , 1, 7-13.

Indian Cybercrime Reporting Portal. (n.d.). National Cybercrime Reporting Portal. Retrieved from https://cybercrime.gov.in/ Webform/ CrimeCatDes.aspx

Jurecic, Q., Spera, C., Wittes, B., & Poplin, C. (2016). Sextortion: Cybersecurity, teenagers and remote sexual assaul. Center for technology innovation at Brookings.

Jurecic, Q., Spera, C., Wittes, B., & Poplin, C. (2016). Sextortion: The problem and solutions. Brookings.

Legal Momentum. (n.d.). 9 Tip to prevent Cyber-sextortion. Retrieved from https:// www. legalmomentum.org/ sites/default/ files/reports/9%20Tips%20to%20Prevent%20 Cyber-Sextortion.pdf

Leukfeldt, D. R., & Malsch, P. M. (2018). Cybercrime has serious consequences for its victims. Netherlands Institute for the study of Crime and Law Enforcement .

Maharashtra Cyber, Home Department. (2020). Cyber Security Awareness for Citizens. India: PricewaterhouseCoopers.

Mengle Enter, G. S. (2018). 'Sextortion', now a reality in India. The Hindu .

Microsoft News Center India. (2017). Digital Civility Index. India: Microsoft.

Mihindukulasuriya, R. (2019). How to save your child from sextortion on Instagram. ThePrint .

Motsomi, K., Makanjee, C., & Nyasulu., P. (2016). Factors affecting effective communication about sexual and reproductive health issues between parents and adolescents in zandsprit informal settlement, Johannesburg, South Africa. The Pan African Medical Journal. , 25, 120.

Nayar, S. (2015). Blackmail, rape, arrest of 3 law students has campus in turmoil. Indian Express .

O'Malley, R. L., & Holt, K. M. (2020). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence. Retrieved from https://doi. org/ 10.1177/ 0886260520909186[Last accessed on 09.03.2020]

Orick; Herrington; LLP Sutcliffe; Legal Momentum. (2016). A call to action: Ending "Sextortion in the Digital Age". U.S.A: Thomas Reuters Foundation.

Robertiello, G., & K. J. (2007). Can we profile sex offenders? A review of sex offender typologies. Aggression and Violent Behavior , 12(5), 508-518.

SCCJR. (2016). Theories and causes of Crime. Scotland: University of Glasgow.

Speier, J. (2019). Reps. Speier and Katko introduce Bipartisan bill to address online exploitation of private images. . Retrieved from https://speier.house. gov/ 2019/5/reps-speier-and-katko-introduce-bipartisan-bill-address-online

State v. Stancl, No. 2009CF000134. (Wis. Cir. Ct. 2009).

Thorn. (2017). Sextortion. U.S.A.: Thorn.

Turnball, T. (2012). Communicating about sexual matters within a family: Facilitators and barriers. Education and Health , 2, 40-47.

United Nations Office on Drugs and Crime . (2015). Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children. Vienna: English, Publishing and Library Section, United Nations.

United States v. Beckett, 369 F. App'x 52 (11th Cir 2010).

United States v. Hutchinson , 588 F. App'x 894 (11th Cir. 2014).