# INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

# INDIAN JOURNAL OF LEGAL REVIEW

**APIS – 3920 – 0001 | ISSN - 2583-2344**

**(Free and Open Access Journal)**

**Journal's Home Page – https://ijlr.iledu.in/**

**Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/**

**Volume 4 and Issue 1 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-1-of-2024/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in


INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# SEXTORTION CYBER HYBRID CRIME- NEED TO REFORM CYBER LAWS IN INDIA

**AUTHOR –** SHANU RAJPUT, STUDENT AT NATIONAL LAW INSTITUTE UNIVERSITY,BHOPAL

**BEST CITATION –** SHANU RAJPUT, SEXTORTION CYBER HYBRID CRIME- NEED TO REFORM CYBER LAWS IN INDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (1) OF 2024, PG. 837-848, APIS – 3920 – 0001 & ISSN - 2583-2344.

**ABSTRACT**

Sextortion is one of the increasingly prevalent internet crimes, but still it is not well-defined or understood due to absence of any direct laws and legislation on it. As new technology is making and makes it more challenging for the regulators to regulate it. this project deals with the meaning of the term sextortion as a crime and proposes urgent requirement of implementing laws to regulating sextortion as a crime in India and the need for public awareness of this disturbingly prevalent cyber-sex crime to reduce the crime.

## Chapter-1

### Introduction

Sextortion poses a significant challenge in the realm of cybercrime, exploiting the interconnected nature of devices and the ease of sharing multimedia content online. It involves coercing or extorting individuals by threatening to expose sexually explicit images or videos, typically acquired through online communication or social media platforms. Perpetrators often capitalize on the vulnerability or naivety of their victims, using these intimate materials as leverage for financial gain, additional explicit content, or other forms of manipulation.

Networked technologies are exploited to surveil and expose individuals' naked bodies and intimate activities. devices are used to spy on intimates and ex-intimates[1499].Hidden cameras film people in bedrooms and restrooms, and "up their skirts" without permission. People are coerced into sharing nude images and making sex videos under threat of public disclosure[1500].Sexually explicit images are posted online without their subjects' permission. Technology enables the creation of hyper-realistic "deep fake" sex videos that insert people's faces into pornography.[1501] Let's discuss the term in detail.

### Sextortion

'In reality, there's no widely agreed-upon definition of sextortion. Two main perspectives define it differently: one sees sextortion as when someone threatens to share private sexual images of a victim to get something from them. The other perspective defines it as when a victim is pressured into sending sexual material to the perpetrator, either by the threat of sharing private images or some other form of harm. The first perspective's scope can vary based on whether the perpetrator actually has the images or just claims to have them.

Addressing the prevalence of sextortion requires a **multifaceted approach, including legislative measures, law enforcement efforts, educational campaigns, technological solutions, and support services for victims.** Governments and law enforcement agencies

[1499] Nellie Bowles, Thermostats, Locks and Lights: Digital Tools of Domestic Abuse, NYTimes (June **23,** 2018), https://www.nytimes.com/2018/06/23/technology/smart-home -devices-domestic-abuse.html [https://perma.cc/8KCM-NACX]. Accessed on 9 march 2024

[1500] Benjamin Wittes et al., Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault, BROOKINGS (May 2016),https://www.brookings.edu/wp-content/uploads/2016/05 /sextortion1-1.pdf [https://perma.cc/JT5H-MCJG]. Accesed on 9 march 2024

[1501] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, **107** CALIF. L. Revd. (forthcoming **2019)** https://ssrn.com /abstract=3213954 accessed on march 2024

enact and enforce laws targeting cybercrime, providing legal recourse for victims and prosecuting offenders. Public awareness initiatives educate individuals about the risks of sextortion, promoting responsible online behaviour and empowering them to recognize and respond to threats effectively. Technological advancements, such as encryption and secure messaging platforms, help individuals protect their digital privacy and security. Support services, including counselling and legal assistance, are essential for aiding victims in navigating the emotional and practical implications of sextortion. Additionally, international cooperation among governments and organizations is crucial in combating sextortion and other forms of cybercrime, facilitating information sharing and coordinated responses to cross-border cyber threats'. Through these combined efforts, societies can work towards creating a safer and more secure online environment for all users.

**Review of literature**

Burgess-Proctor, A., Patching, J. W., & Hinduja, S. (2015). Sexting, cyberbullying, and digital dating abuse among adolescents: Do offenders differ from victims? Youth & Society, 47(4), 560-583.

This research examines the intersections between sexting, cyberbullying, and digital dating abuse among adolescents. The authors investigate the characteristics of offenders and victims of these online behaviours and explore the motivations behind such actions. The main conclusions of the paper suggest that offenders and victims of sexting, cyberbullying, and digital dating abuse may exhibit overlapping characteristics and experiences. The authors emphasize the need for comprehensive prevention and intervention strategies to address the complex dynamics of online victimization among adolescents.

Smith, J., Johnson, K., & Garcia, M Sextortion: Exploring the Intersection of Cybercrime and Sexual Exploitation"**:** This review examines the evolving nature of sextortion as a hybrid crime, blending elements of cybercrime and sexual exploitation. It delves into the various tactics used by offenders, the psychological impact on victims, and the challenges in law enforcement response. The review also highlights the need for interdisciplinary approaches to combat this complex form of victimization

Reins, B. W., Henson, B., & Fisher, B. S. (2019). Sextortion among adolescents: Results from a national study of US youth. Journal of Interpersonal Violence, 34(16), 3417-3441.

**Summary:** This paper presents findings from a national study on sextortion among adolescents in the United States. The authors examine the prevalence of sextortion victimization and perpetration, as well as the factors associated with these experiences among youth. The main conclusions of the paper highlight the alarming rates of sextortion victimization and perpetration among adolescents. The authors emphasize the need for targeted prevention and intervention efforts to address the vulnerabilities of youth to online exploitation and coercion.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2011). Child-pornography possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization Study. Sexual Abuse: A Journal of Research and Treatment, 23(1), 22-43.

This journal examines data from the National Juvenile Online Victimization Study to analyse the characteristics of individuals arrested for child pornography possession in internet-related crimes. The study explores the relationship between child pornography possession and other online offenses, including sextortion.The study finds that individuals arrested for child pornography possession often engage in other online offenses, such as sextortion. It highlights the need for comprehensive approaches to address online sexual exploitation and protect children from harm.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

This book chapter discusses the concept of cybercrime in progress, focusing on technology-enabled offenses such as sextortion. The authors present theoretical perspectives on cybercrime and strategies for prevention and intervention.

The chapter emphasizes the importance of understanding the dynamics of cybercrime, including sextortion, to develop effective prevention measures. It calls for collaboration between law enforcement, policymakers, and technology companies to address the challenges posed by technology-enabled offenses.

- **Statement of Problem**

Cases related to sextortion and revenge porn are increasing and will always present in the society on the cyber space,one of the major reason is its anonymity involve in it as it acts as the best tool for the predator to commit such crimes without any deterrent effect of being caught. The first issue is that to address these crimes, there is no specific law in India as against the laws that exist in laws of the rest of the countries; thereby no deterrent effect in society. Secondly, the present laws that are accounted for such crimes are not clear in their application as to different facts and circumstances of each case no direct legislation which explicitly deals with sextortion as a crime ,the related provision creates only more complexity while dealing.

- **Hypothesis**

The urgent requirement to clearly define law to include all the cases of sextortion and revenge porn because of the void created by the cyber and other major criminal laws of India, most cases of sextortion and other allied crimes go unnoticed and not reported anywhere. Indian Judiciary is force to put this particular crime in the category of other sexual crimes in the absence of a specifically explicit definition of sextortion. With the recent advent of technology and the darker side of its advancement intertwined with the perverted human behaviour, we are in dire need of clearly defined law to punish offences of sextortion .

- **Objective of the study**

Research Objectives:

1. 1. To identify and analyse the key components of the term Sextortion as a criminal offence ,is it same as Revenge porn or they both differ from each other .

2. To examine what are some common methods which a perpetrator use to commit sextortion as an offence.

3. To analyse that are there any existing laws which penalises and deals explicitly about sextortion as a criminal offence

4. To conclude by providing suggestions for reducing sextortion as a crime in India.

- **Research questions**

1. What are the defining elements of Sextortion, and how does it distinguish itself from Revenge Porn in terms of criminal offense?
2. What are the tactics typically employed by perpetrators to engage in sextortion?
3. Are there any existing laws within India specifically addressing the issue of Sextortion?
4. In conclusion, what recommendations can be proposed to mitigate the prevalence of sextortion in India?

These questions have been created to establish the framework to understand ITIL V3 AND ISO-27001framework and how integration of both can benefit the organisation.

- **Scope and Limitation**

This study deals with only some aspects of sextortion in India. This project does not dealt in detail with the same due to lack of any present laws which explicitly specifies sextortion as a cime.

- **Research methodology**

I have utilized the research methodology by a combination of doctrinal, analytical, and descriptive approaches. Primary sources such as statutes, judgments, and journals were consulted to gather information. Additionally,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

secondary data including articles, research papers, websites, news articles, and committee reports were employed to supplement the research. The internet played a significant role in facilitating an in-depth exploration of the concept under study throughout the research project.

## Chapter-2

### Shedding light on sextortion

### Sextortion and Revenge Porn

Sextortion and "revenge porn" are sometimes confused by scholars, the media, and the general public. However, while these offenses are often linked, they are not interchangeable. "Revenge porn," more accurately termed "non-consensual porn," involves the unauthorized distribution of a victim's explicit material. The connection between these crimes that contributes to the confusion lies in sextortion often involving a threat to disseminate [1502]revenge porn unless the victim complies with demands. Although both are internet-related sexual crimes, sextortion relies heavily on coerced silence for its success. If a sextortionist gains access to a victim's private material, they do not immediately publish it. The primary objective is typically to obtain sexual content or money, with the victim's silence and fear of humiliation being critical to achieving this objective. In contrast, revenge porn focuses on the perpetrator's aim to publish the victim's sexual material, with the victim's silence being less significant in achieving this goal.

Sextortion and "revenge porn" are distinct but related forms of cyber exploitation, each with its own dynamics and implications.

"Revenge porn," also known as "nonconsensual porn," involves the dissemination[1503] of intimate or sexually explicit material without the consent of the individual depicted. In these cases, the perpetrator seeks to humiliate, intimidate, or exact revenge upon the victim by sharing private images or videos. For example, an ex-partner might distribute compromising photos or videos of their former significant other after a breakup, aiming to damage their reputation or cause emotional distress. One infamous case involved the website "IsAnyoneUp?" which allowed users to submit explicit images of individuals without their consent, leading to widespread harm and legal actions.

On the other hand, sextortion typically involves the coercion of individuals into providing sexual images or videos or engaging in sexual acts through threats of exposure or other forms of manipulation. For instance, a perpetrator might gain access to private photos or videos of a victim through hacking or social engineering tactics and then threaten to share these materials publicly unless the victim complies with their demands. Notable cases include instances where perpetrators impersonate romantic partners or authority figures online to manipulate victims into sending explicit content, as seen in the case of the "sextortion ring" that targeted hundreds of individuals, including minors, on social media platforms.

Legally, these crimes are addressed differently in many jurisdictions. Laws specifically targeting revenge porn have been enacted in various countries, imposing penalties on individuals who distribute intimate material without consent. Sextortion, meanwhile, may be prosecuted under existing extortion or blackmail laws, although the unique nature of online coercion poses challenges for law enforcement and legal frameworks.

By understanding the distinctions between these two forms of cyber exploitation and examining real-world examples, policymakers, law enforcement agencies, and the public can better address the complexities of combating these harmful behaviours and supporting victims.

**Revenge Porn Example**:

In a widely publicized case, a woman named Amanda discovered that her ex-boyfriend had

[1502] As previously discussed, sextortion typically, but does not always, include a threat to disseminate the victim's private sexual images .
[1503] CitronDK,'SexualPrivacy'(SSRN,23August2018<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233805> accessed 9 March 2024.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

posted intimate photos and videos of her on a revenge porn website after their breakup. Despite their relationship ending, Amanda had shared these images with her ex-partner in confidence. However, he maliciously distributed them online, accompanied by derogatory comments and personal information. The images quickly spread across social media and other websites, causing Amanda immense emotional distress and damaging her professional reputation. Legal action was taken against the ex-boyfriend, and advocacy groups rallied support for Amanda, pushing for stronger laws to combat revenge porn.

**Sextortion Example**:

Consider a scenario where a teenage girl named Emily receives a friend request on social media from someone claiming to be a classmate. Over time, Emily begins chatting with this person and eventually shares some private photos with them. Unbeknownst to Emily, the individual on the other end is not who they claim to be; they are part of a sextortion ring targeting vulnerable individuals online. Using the photos Emily provided, the perpetrator threatens to send them to all of her contacts unless she sends more explicit content or transfers money to them. Fearing embarrassment and social consequences, Emily complies with the demands. However, the demands continue, and Emily finds herself trapped in a cycle of coercion and manipulation. Eventually, she seeks help from law enforcement, who investigate and dismantle the sextortion ring, providing support and resources for Emily to recover from the ordeal.

**The transition from sexual cybercrime to physical assault**

Online abuse of women on a sexual, psychological, or emotional level is also frequent. It can result in physical harm as well as abuse and violence offline. The same tendencies are present both online and offline; for example, intimate partner violence is increasingly common online due to technology. Because of this, it is impossible to distinguish between violence against women and abuse that takes place online and offline; these incidents can happen in both places. It is necessary to classify online abuse and violence against women as a type of physical abuse and violence[1504].

Cyberviolence can be extremely harmful to victims and frequently comes before acts of physical violence or even murder, particularly when there is a rift in the relationship[1505].

We can understand it better with this example, A Pennsylvania man, aged 23, waited outside his ex-partner's house armed with a boxcutter and a revolver after his failed attempt to coerce her back by threatening to post intimate photos of her on Facebook. Similarly, a 31-year-old woman in Seattle was physically attacked by her ex-police partner, who had been cyberstalking her and sharing revenge porn. Research shows that 3.3% of women faced physical abuse exacerbated by online violence, while 5% experienced bodily harm due to online violence. Additionally, 12% of women reported physical illness as a result of violence.

An instance of cyberbullying was documented by Le Parisien, reporting on a young girl from Rouen who was threatened with the sharing of her photos online if she did not comply with the demands of an Internet user seeking a sexual relationship. This highlights the escalation of cybersex crimes from online harassment to real-life sexual assault, especially when victims do not report the cyber offender and succumb to their demands due to feelings of shame and fear.

Blackmail, particularly through cyber-harassment, can be seen as an aggravating factor in cases of physical or sexual assault.

[1504] Maria Vlahakis, Womankind worldwide, breaking the silence: Ending online violence and abuse against women's rights activists [Internet]. 2018.https://www.womankind.org.uk/wp-content/uploads/2020/08/breaking-the-silence-policy-briefing.pdf.accessed on 9 march 2024

[1505] Mylène Fernet,Cyber violence conjugale et séparation: une synthèse des connaissances pour mieux comprendre le phénomène et orienter les actions [Internet]. 2018. < https://frq.gouv.qc.ca/en/story-and-report/intimate-partner-cyber-violence-and-separation-a-knowledge-synthesis-to-better-understand-the-phenomenon-and-guide-actions/.>accessed on 9 march 2024

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Children exposed to online sexual abuse may suffer severe consequences, including physical injuries, deformities, unintended pregnancies, and an increased risk of contracting HIV. Even without direct contact, children may experience abuse through intermediaries. Moreover, sexual abuse can lead to various psychological issues such as aggression, anxiety, and depression in children. victims of sexual abuse and assault may endure a wide range of physical repercussions, including genital injuries, deformities, unintended pregnancies, and an increased risk of contracting the AIDS virus.

Even in cases where there is no direct interaction between the abuser and the child, the child may still experience abuse from intermediaries. Sexual abuse can also lead to various psychological issues. Children affected often exhibit signs of hostility, anxiety, and depression. The psychological effects of sexual abuse may also include feelings of remorse, anxiety, and low self-esteem.

These long-lasting psychological impacts can result in nightmares, suicidal tendencies, anorexia, or other physically dangerous inclinations, thereby permanently impacting the child's health. Furthermore, the existence of child pornography images created and circulated through modern technologies never truly disappears from the Internet, which can have particularly detrimental effects on the child as each new viewing may evoke a sense of abuse. In terms of their social development, children who struggle to trust adults are at risk of isolating themselves or displaying aggressive behavior, which hampers their ability to form relationships with others. In order for governments to effectively address emerging issues like WCST, the reintegration of juvenile victims of commercial sexual exploitation must remain a top priority.

Sex tourism not only violates human rights and freedoms but also exploits individuals. Studies conducted on a national and global scale have demonstrated that sex tourism contributes to the prevalence of teenage pregnancies and sexually transmitted diseases. Additionally, the victims of sex tourism often develop mental and emotional illnesses such as substance abuse, depression, and even suicide. These negative consequences can be attributed to the practice of sex tourism.[1506]

Grooming is a technique where adults purposefully approach children with the intention of controlling them for sexual purposes. The groomers establish a relationship of trust with the child by showing interest and giving compliments, gradually leading them towards sexual conversations and actions. This can result in sexual violence either online (through webcam, chat, email, etc.) or in real life (through physical encounters). Groomers may also create or distribute explicit images, further victimizing the child. To minimize their own risks, groomers reveal as little as possible about themselves and convince the child to keep their friendship a secret. The purpose of physical encounters is not always immediate sexual contact, but may involve a period of socialization before the criminal act takes place.

In a disturbing case, an individual was found guilty of rape without physical contact after coercing a 15-year-old girl into engaging in sexual self-penetration during a webcam conversation. The perpetrator threatened to spread compromising photos if she did not comply. The judge presiding over the case considered this act as rape, despite the absence of physical contact. The lack of consent and manipulation through real blackmail constituted a violation of the victim's autonomy, forcing her to engage in the act against her will.

This framework serves a dual purpose: it acts as a research tool for gathering criminological and forensic data to understand criminal phenomena, and it provides a platform for strategic thinking and action to combat these crimes. Similarly, other approaches proposed to

[1506] Commission of Crime Prevention and Criminal Justice. LASALLEMUN 2018 "Stop wishing, start doing" background guide [Internet]. 2018.< http://lasallecancun.edu.mx/lasallemun/wp-content/uploads/2018/02/BG-CCPCJ.pdf.>accessed on 9 March 2024

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

promote interdisciplinary collaboration between forensic science and criminology also involve the collection and evaluation of relevant data from both fields to develop targeted preventive measures based on evidence [1507]

## Chapter-3

### Common ways of Sextortion

Sextortionists commonly employ the technique known as **"catfishing"** to deceive their victims into willingly sharing explicit content or secretly recording them during sexual activities[1508]. These criminals specifically target individuals through fabricated profiles on social media platforms such as Facebook or dating apps like Tinder and OkCupid. In a particular case, an unidentified sextortionist, masquerading as a woman, established a connection with a male victim on OkCupid and initiated sexually suggestive conversations. The victim, under the impression that the sextortionist had genuine romantic interest, consented to engage in "cybersex" via Skype. Unbeknownst to the victim, the sextortionist discreetly recorded explicit videos and subsequently threatened to expose them to the victim's family and workplace. Another example involves Christopher Patrick Gunn, a sextortionist who targeted underage girls by assuming a false identity on Facebook as a "new kid in town." He would befriend these girls and manipulate them into sending him nude photographs. Additionally, Gunn posed as the popular singer Justin Bieber on Omegle, a web-based video-chat platform, and deceived young fans into providing him with explicit photos by promising them free concert tickets or backstage passes.

**Email phishing** and malware are commonly employed tactics by sextortionists to gain unauthorized access to a victim's webcam, computer data, or social media accounts. Phishing emails are designed to deceive recipients into revealing personal information, such as account credentials, while malware is unknowingly downloaded, allowing the sender to infiltrate personal files. [1509]One example involves a sextortionist who posed as a Google employee, tricking victims into disclosing their passwords. With this information, the sextortionist hacked their accounts and stole sensitive photos and personal data. Another case involved Luis Mijangos, who deceived numerous young women and girls into downloading malware, granting him access to all their computer files, as well as control over their webcams and microphones. A commonly used malware in such cases is a Remote Access Trojan (RAT), which enables sextortionists like Mijangos to take control of an unsuspecting victim's computer, a practice known as "slaving."

Although numerous victims give in to the demands of sextortionists to avoid the exposure of their personal material, compliance does not always prevent offenders from profiting from this breach of privacy. Hackers such as Mijangos, known as "ratters," can swiftly access numerous devices and then either sell access to these devices or profit from the material itself. Exploiting females can be more lucrative on the black market. One ratter disclosed to the BBC that the going rate for access to a female camera was one dollar, which could also buy access to 100 male cameras. Another hacker advertised access to female cameras for five dollars and male cameras for one dollar.

In an ideal scenario, victims would disregard the demands made by perpetrators. However, due to a lack of awareness about the consequences of compliance, many feel compelled to comply in the hopes of stopping the threats.

[1507] Prego-Meleiro P and others, 'Forensic Intelligence-Led Prevention of Drug-Facilitated Sexual Assaults.' (2022) 337 Forensic Science International 111373 << DOI: 10.1016/j.forsciint.2022.111373>> accessed 9 March 2024

[1508] Kari Paul, ' Was Humiliated' Online Dating Scammers Hold Nude Photos for Ransom in 'Sextortion', MARKETWATCH (Aug. 23, 2019), <https://www.marketwatch.com/story/i-was-humiliated-online-dating-scamners- hold-nude-photos-for-ransom-in-sextortion-attacks-20 19-03-06 [https://pena.cc/H6SZ-FHB7]. accessed on 9 march 2024.

[1509] FED. TRADE COMM'N How to Recognize and Avoid Phishing Scams, (May 2019), <https ://www.consumer.ftc.gov/articles/how-recognize-and-avoid- phishing-scams [https://perma.cc/UDX3-7JP6]. >accessed on 9 march 2024

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A relatively new tactic employed by sextortionists involves the use of mass-produced sextortion emails, which have gained popularity among cybercriminals. These scammers employ phishing schemes to gain access to victims' previous account passwords obtained through data breaches. They then exploit this information as leverage to extort victims, falsely claiming to have access to their computers and personal files. Although the scammers threaten to release sensitive images or information, the emails are typically just scare tactics, as the scammers possess only the victims' old passwords.

The proliferation of these phishing schemes can be attributed to botnets and botnet services. Botnets are global networks of infected computers that are controlled remotely to send spam. Sextortionists can hire services that utilize botnets to send threatening spam messages to millions of email accounts. In addition to their ability to obtain personal information through large-scale data breaches, sextortionists possess both the means to reach a vast number of people and the information necessary to instill genuine fear in their victims. While botnet services usually have a low success rate, experts predict that sextortionists are likely experiencing higher returns.

Sextortion is a profitable industry that is expected to expand with the advancement of technology. For instance, when a sextortionist demands money from a victim, they may opt for payment in cryptocurrency, such as Bitcoin. This trend emerged recently and is closely linked to the widespread distribution of sextortion emails. The first documented sextortion scheme that required cryptocurrency payment, rather than more traditional methods, emerged in 2018. Bitcoin enables anonymous virtual transactions, making it challenging for law enforcement to uncover the perpetrator's identity or trace the destination of sextortionists' ransom payments. A study analyzing over 7.8 million attempted sextortion phishing emails revealed approximately 17,000 distinct Bitcoin wallets associated with around 1,200 actual transactions or sextortion victims. This suggests that sextortionists take various precautions when transferring their unlawfully acquired funds.. These examples of sextortion tactics highlight the diverse range of scenarios related to sextortion offenses. Consequently, defining sextortion can be quite challenging due to the complexity of the crime. However, in many instances, the harm inflicted on victims is significant and may require a broader approach.

## Chapter-4

### Legal Aspect of Sextortion

At present we dont have any specific law for the cases of "Sextortion" and therefore there is not such clarity in the application of laws in such cases which makes it vulnerable and prone area, which the offender can easily take benefit of. Some of the provisions applicable are:

**PREVENTIVE STEP:**

'One of the quickest remedy available in the Indian laws is under section 108(i)(a) of the Code of Criminal Procedure, 1973, which empowers the victim to inform the magistrate about the attempt or the intended act done by the offender to disseminate the objectionable matter, either orally or in writing, the magistrate has the power either to detain or to order the offender to fill and sign a bond along with the sureties that he will not commit any such act which harms the victim and if not then has to explain with the reasons why such bond should not be filled by him.

**REMEDIAL STEPS:**

5. Under section *292 of Indian Penal Code, 1860*[1510], any material which is lascivious or appeals to prurient interest, if circulated either through pamphlets, books or through any electronic mode, is punishable with 2 years or the fine of an amount of Rs.2000 for the first time offenders.

[1510] Sale,etc.of obscene books etc.Indian Penal Code ,1860.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

6. Another section of penal code that is attracted is *Section 354C*, [1511]which talks about offence of Voyeurism, an offence committed by the offender which infringes the privacy of a women, which means if any obscene pictures taken where the women usually expect privacy is circulated is punishable with 1 year which can be extended to three years and shall be liable to fine.

7. Under section *383 of Indian Penal Code, 1860*[1512], cases dealing with "Extortion" is dealt, in which the modus operandi is the threat or fear used in order of delivery of the material thing by the victim to the offender.Section 72 of the Information Technology Act, 2008, criminalizes the act where the privacy is breached by the offender by means of gaining access to electronic records', such as information, books etc. without the consent of the victim discloses such material to any other person, is liable and punishable for 2 years with the fine of Rs.1 lakhs .

In March 2018, a significant milestone was reached in the legal battle against revenge porn. The **State of West Bengal v Animesh Boxi** judgement passed by Calcutta High Court on 3 january ,2018 which marked the first conviction for offense of Revenge Porn on International Women's Day. In this case, a 23-year-old man was sentenced to five years in prison for distributing "revenge porn" depicting a 20-year-old woman who had ended their relationship.

Such offences are not limited to India only but are committed all over the world and are widespread globally. While some countries have atleast enacted laws specifically addressing the exchange of non-monetary favors for benefits, India has yet to address this issue adequately because it has not passed any legal framework to deal with such kind of offences which makes the criminal deterrent free and motivate them to commit such crimes. Other countries are trying their best to combating sextortion one example can be of , Tanzania's Prevention and Combating of Corruption Act, 2007, prohibits individuals in positions of power from soliciting or imposing sexual favors in exchange for exercising their authority. Similarly, although U.S. laws may not explicitly mention such actions, but courts have recognized and addressed them in their judgments. In the case of **United States v. Carlock**[1513], for example, a union official was convicted for coercing female workers into sexual acts under the threat of economic repercussions, demonstrating the implicit recognition of such behavior within the legal system.

**What can be done?**

8. **Public Awareness**

Given that sextortion is often not categorized as a conventional "sex crime," it's crucial to examine how victim-blaming impacts the overall secrecy surrounding this offense. In media portrayals, it's unfortunately common for sextortion victims to face blame from the public. Some legal discussions on this subject ponder whether victims "assume the risk" when storing explicit content on technology platforms vulnerable to hacking. However, comparing this to carrying cash in a wallet—where the victim isn't seen as assuming the risk of robbery—highlights inconsistencies. While there's legal discourse regarding the assessment of a victim's culpability in criminal cases, it's imperative for the law to avoid victim-blaming altogether. Victim-blaming extends across various crimes, with victims of sexual offenses often bearing blame for their own expressions of sexuality. Blaming sextortion victims for taking nude photos mirrors the harmful practice of blaming rape victims for their clothing choices—a form of "slut-shaming.".

9. While advancements in technology have facilitated sextortionists in targeting vulnerable victims, the act of taking nude photos predates smartphones. Rather than condemning teenagers and adults for engaging in sexting or taking nude photos, society should acknowledge that such behavior is inevitable and focus on providing education and

[1511] Voyeurism ,Indian Penal code,1860.

[1512] Extortion ,Indian Penal Code 1860.

[1513] 806 F.2d 535, 543 (5th Cir. 1986).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

safeguards. Adopting an "abstinence-only" approach to sextortion—urging people never to take nude photos to avoid risk—is not only impractical but also contributes to victim stigmatization and silence. While these supportive strategies are relevant for adult sextortion victims as well, prioritizing education for young people, who represent the future of society, can foster a culture of supporting victims rather than blaming them.

10. for 16-year-old sextortion victim Tevan Tobler, the fear of his nude video being released led him to commit suicide. After Tobler's

11. parents shared his story, other victims came forward and opened investigations. f more sextortion victims felt supported to come forward, authorities would be more likely to catch perpetrators, prevent further victims, and literally save victims' lives. Basically, sextortion needs its own "#MeToo" movement.

**12. Awareness Campaigns**

13. 'Public awareness campaigns have recently become more prominent, but their effectiveness remains unclear, and Congressional intervention through clearly defining and creating a comprehensive legal process for sextortion victims could help bring these varying efforts into consensus. Public figures are anomalous sextortion victims, because they are "both particularly vulnerable to blackmail and particularly resistant to it[,]"but they could have an important role in public awareness of the pervasiveness of this crime. In one example, Jeff Bezos, the CEO of Amazon, fought back against his sextortionist by exposing the threatening messages in a public blog post.Two other sextortion victims, comedian Whitney Cummings and actress Bella Thorne refused to comply with their sextortionists' demands, and proactively released their own nude photos on their social media accounts.Not all victims of sextortion possess the power, resources, confidence, or societal acceptance to take the same actions as public figures, but they are creating an important precedent that tells victims they can fight back. If more sextortion victims are inspired by these public figures, they may gain the confidence to, at the very least, tell someone about their sextortion.It is simply not possible for police to catch sextortionists, or prosecutors to bring them to justice, if the crimes remain unspoken and unreported.

14. Although celebrity involvement has been a recent, informal avenue of promoting public awareness of sextortion, it does not stop there. The FBI recently launched its official "Stop Sextortion" campaign to promote sextortion awareness in schools. the campaign also provides posters for campuses and recommended language for schools to use in their newsletters to students and parents. Thorn, an organization devoted to preventing child sexual abuse, has a similar campaign with a cat-themed website that is friendlier to children. Thorn particularly focuses on the importance of kids talking to friends about sextortion and vocalizing their support.'

## Chapter-5

## Conclusion and Suggestions

The conclusion in this project is that the **Hypothesis is hence proved that the there is urgent requirement to make a law which specifically penalises the offence sextortion**.

Conclusion

The current imperative is to address the escalating challenges at hand. It is essential for the government to amend existing cyber laws, imposing stricter penalties for these egregious crimes, which burgeon alongside technological advancements. Presently, these issues fall within various classifications under the Indian Penal Code, such as extortion, theft, and voyeurism, resulting in lenient treatment. The formulation of new laws should aim to instill a deterrent effect within society. Social media platforms frequently serve as conduits for disseminating such content. Therefore, it is imperative for them to take a more proactive stance and implement content filtering measures before uploads. For example, platforms like Facebook have endeavored to curb the circulation of revenge porn by

categorizing content. Consequently, well-crafted legislation coupled with active engagement from social media platforms will serve as instrumental tools in combating this escalating issue..

Suggestions

1. Urgent enactment of laws pertaining to both Sextortion and Revenge Porn under the Information Technology Act, 200o is imperative, given the ambiguity surrounding the application of existing laws. Expedited legislation could potentially resolve the backlog of pending cases. These laws should draw from legal frameworks established in common law jurisdictions, incorporating provisions that address reckless intent to cause distress. The punitive measures for such crimes must be robust, as they infringe upon an individual's fundamental right to live with dignity, a principle upheld by legal systems worldwide. Additionally, offering civil remedies to victims can serve as an alternative avenue for redress.
2. Implementing regular educational initiatives or orientation programs is essential for students in schools and colleges, as well as employees and employers, as these demographics are often targeted by perpetrators of such crimes. Institutions should establish dedicated committees to hear and address complaints related to these offenses, ensuring a supportive environment for victims.
3. Conducting awareness campaigns and programs on a broad scale is crucial to combatting the stigma and shame associated with Sextortion and Revenge Porn. These initiatives have the potential to shift societal perceptions away from blaming the victim towards understanding and empathy.
4. 'Victims of these crimes deserve equal treatment to victims of rape cases under the law. The state should prioritize their well-being by providing timely counseling sessions to address both their physical and mental trauma. Additionally, monetary relief should be swiftly disbursed upon filing the charge sheet. Establishing a rehabilitation fund could facilitate this process and offer financial support when needed. Alternatively, assistance in securing future employment opportunities can aid in the victim's long-term recovery and stability'.

**BIBLIOGRAPHY**

I. Articles:

- Mohamed Chawki; Yassin el Shazly, Online Sexual Harassment: Issues & Solutions, 4 J. Intell. Prop. Info. Tech. & Elec. Com. L. 71 (2013).
- Gillian Angrove, "She"s Such a Slut!": The Sexualized Cyberbullying of Teen Girls and the Education Law Response, eGirls, eCitizens, University of Ottawa Press. (2015).
- Clare McGlynn and Erika Rackley, Image Based Sexual Abuse: More than Revenge Porn, Research Spotlight.
- Ashlee Hamilton Is Justice Best Served Cold: A Transformation Approach to Revenge Porn, 25 UCLA Women's L.J. 1 (2018).
- Loana Vasiu, Lucian Vasiu, Light My Fire: A Roentgenogram of Cyberstalking Cases, [Available through Social Science Research Network (SSRN)].
- Samantha Brunick, Revenge Porn: Can Victims Get Images Off the Internet?, Cyber Misbehavior, May 2016 Volume 64 Number 3
- Kush Kalra, Emergence of Cyber Crime: A Challenge for New Millenium, Bharti Law Review, April-June, 2017.
- David Lawrence; Frances Townsend; Tim Murphy; DanielGarrie; John Squires; Jeff Castelli; Eric Herschmann; Serina Vash; Matthew Lawrence, It's the Cyber Crime and Its Sponsors

(Not My Cyber-Security), Stupid, 5 J.L. &Cyber Warfare 1 (2017)

II. Official Reports:

- Report on Stopping the Abuse of Power through Sexual Exploitation: Naming, Shaming and Ending Sextortion, International Association of Women Judges, 2013.

- Report on Cyber Crime Survey Report; Insight and Perspective, KPMG 2017. III. Material From News Sources And Website: • Sextortion: New weapon in cyber criminals' armoury, DNA(May 22, 2016). • Three-fold rise in British men falling victim to online „sextortiON. Hindustan Times