

Digital Abuse and Cyber Threats: With Reference to Revenge Porn and Sextortion

Ms. Savina R. Crasto

Research Scholar, Department of Law, DACN, Nagpur, India
advocatesavinacrasto@yahoo.com

Abstract: *The expression “revenge porn” may be misleading as it implies that, as the target, the person has done something to deserve this treatment. One may have shared personal photos with a partner, only to later find those images anonymously posted on an online forum. Image-based sexual abuse is stimulated by the desire to maintain control or the perpetrator has a vengeful motive. The perpetrator may be trying to compel you to continue with the relationship by threatening to share the images or perhaps they’re seeking to “punish” the person for leaving the relationship or some other realised wrongdoing. Being the target of revenge porn is itself a form of sexual abuse. One feels violated and is left with no sense of control over the situation. The sudden loss of privacy can make one feel exposed, ashamed, and terrified to go out in public. Feelings of guilt can even prevent one from reaching out to loved ones for support thereby leading to social isolation which can impact one’s day-to-day health. Even if the pictures are removed from online spaces, there is always a fear that they could reemerge at any time.*

In case someone threatens to release private images or videos unless the person meets their demands is known as sexual extortion or “sextortion.” This is a serious cybercrime where the perpetrator attempts to blackmail you either for money or sexual favors.

In this paper we will deal with revenge porn and sextortion as a form of sexual abuse and the ways to cope with the effects of online harassment mainly by report cybercrime and practicing safe sexting.

Keywords: revenge porn, privacy, sextortion, punish, sexual abuse

I. INTRODUCTION

We are continuously striving, as a community, to adapt to terms that are easily, constantly and hypercritically evolving including technology-facilitated forms of sexual abuse. As and when possible, we try to avoid using the terminology used by the perpetrators of abuse and rather seek to use terms that directly convey the nature and the detriment of the abuse. Since the words used are important in such online abuse, we must use survivor-centered language. For the first time in history, global connectivity of the Internet means that you don’t have to be in the same country as someone to sexually menace that person.

Revenge Porn is when someone shares, or threatens to share, private, sexual images or videos of a person without his/her consent. This is a criminal offence and those sharing these images without consent must be prosecuted. Increasingly, we see perpetrators engaging in revenge porn, either to take revenge against the ex-partner, or compel him or her to stay, or to obtain money, control of joint assets, or favorable divorce or custody settlements.

The term ‘revenge’ suggests that the perpetrators are primarily motivated by personal vengeance. However, the fact of the matter is that, perpetrators may be motivated by a range of factors, like a desire for profit, entertainers may also be for no particular reason at all. The constant factor is the lack of consent in its distribution. The usage of the term ‘porn’ too is to some extent misleading, because though the creation of intimate and explicit videos and photographs in a private space in a consensual relationship may not be correctly labelled as pornography, their non-consensual distribution and publication transforms them into a sexual entertainment for public consumption, which is to be treated as pornography.

Yet another form of image-based sexual abuse is the usage of intimate images to threaten, coerce or extort victims. Sextortion, a combination of two words “sexual” and “extortion,” is the offence of distributing intimate, sexual materials unless a victim complies with the illegal demands. For example, a predator who obtains some intimate

material will demand their target to provide even more explicit material under threat that they will distribute the images they have via the internet. Further cyber sextortion is a specie of image-based sexual offence in which images are used for inflicting harm. In spite of the serious nature of these crimes, there is a dearth of empirical knowledge of sextortion. The different nature of cyber sextortion has counteraccusations for crime control policies. Certain offenders are more likely to be restrained and prosecuted depending on the crime, the victim and the methodology. In addition, there has been a lack of legislative action targeting cyber sextortion, which limits legal expedient available to the victims. This paper explores the offence of revenge porn and sextortion as a form of Digital Abuse and Cyber Threat, its impact on the victim, the challenges in addressing it and the tools and strategies being used to combat this alarming trend. Hence, there is a need to consider the aftermath of revenge pornography and sextortion and to understand it in terms of the differences, red flags, awareness level, role of consent, etc. including its impact on victims.

Revenge Porn & Sextortion

The concept of revenge porn began in the year 1980s and quickly evolved into a widespread issue at the turn of the century when cell phones and user generated content (UGC) websites became widely adopted by the general public. Due to the spread of sexual image based abuse, states have begun to enact criminal statutes and/or allowing victims to recover damages under existing civil causes of action. The laws, however, differ from state to state and revenge porn continues to be a recent phenomenon in the context of the existing legal landscape.

As the laws evolve, so does technology. Similarly, revenge porn in the traditional sense started as image based abuse between partners in an intimate relationship and quickly evolved into a larger issue. Hackers began to access private devices of others, steal intimate photos, threaten victims and also publish photos on the internet.

The offence of revenge porn can take place both online and offline and is mainly done in order to cause embarrassment or distress. However, the main aim is to take 'revenge' on a partner after a break-up. In the recent years, the issue of revenge porn has gained attention as a form of online harassment and violation of privacy. Thus, revenge porn is less about revenge and more about the infringement of privacy and hence it should be termed as non-consensual pornography, since the essence of it is leaking private images without the consent of the victim.

On the other hand Sextortion is not necessarily about revenge. The content may be shared, or threats may be made to share such content, as and by way of financial extortion or blackmail. Predators often, in their initial contact with a young person, send them friend requests and approach teens with compliments or flattery words. They may also promise a romantic relationship. They then start what appears to be like a genuine conversation to strike up a close friendship with their victim. These criminals very often make the first contact with a victim on one platform, then ask them to move to a second or third platform that uses encrypted messaging to make tracking their crimes difficult.

Though sextortion may come in a multitude of forms, it typically begins when you meet a stranger online, most commonly through social media, online dating website or a messaging app. However, before one even realizes that they are being extorted, the perpetrators have already done their research on you – on where one lives and works, the marital or relationship status and other information they intend to use to victimize a person. One of their favorite tactics is to take screenshots of the victim's friendlist on Facebook, Instagram, etc. The scheme's success is entirely dependent on one's fear and panic, as well as the victim's ability to pay. Vulnerability and capability are the two traits in victims which the criminals look out for besides the others. Their plan fails if the victims are not both vulnerable to their threats and capable of paying their demands. The victims who demonstrate both traits earn the strong focus and attention of the perpetrators of the scheme.

Sextortionists record and preserve entire chats and videos. They also visit public social media profiles to find out more about their victims, going through friend lists and gathering other personal information that may harm their target's reputation.

Difference between Revenge Porn & Sextortion

Revenge Porn

1. **The Perpetrator:** This is an ex-partner or someone who that partner is associated with.

2. **Motive: Here the motive is** to humiliate, shame or emotionally hurt the victim, so as to take revenge. Many a times, victims are not even aware that their images have been leaked and are only informed incase their friends or family members discover the images online.
3. **Consent: These videos and photos may have been initially taken with consent. However, sharing the same is not something for which the consent was given. It may also be that** the intimate material was probably shared consensually in the past without coercion or may be through catfishing. However, consent obtained if the victim did not give consent for the images to be shared with anyone else, the act of sharing the content would be considered illegal.
4. **Source of the Leakage:** These images of videos are often placed on different platforms including porn sites or social blogs where revenge porn content is not monitored well.
5. **Legal Framework:** In many countries, it is considered as a crime of abuse or privacy violation. Many countries have introduced laws that specifically aim at preventing the sharing of non-consensual intimate images under the heading “revenge porn laws.”
6. **Impact on the Victim:** The most obvious impact would be the reputational and emotional harm to the victim; some victims may even be subject to harassment by viewers who observe their content where it is posted.

Sextortion

1. **The Perpetrator:** These are strangers or cybercriminals using fraudulent digital personas designed to catfish the victim.
2. **Motive:** The criminal seeks to extort money from the victim. By using the fear of exposure the perpetrator will promise to delete the content if the victim pays them, though this is normally a tactic to create compliance with additional demands.
3. **Role of Consent:** Since the images were obtained through fraud and coercion, the criminal does not have any rights to the images.
4. **Source of the Leakage:** Most cyber blackmailers that conduct sextortion scams will threaten to release the content to the victim’s connections on different social platforms. They also create group messages with a threat of clicking the send button if their demands are not complied with.
5. **Legal Framework:** Extortion or any other acts that are classified as extortion are considered illegal in virtually every country. Universally it is recognized as a crime as it violates the basic principles of personal rights. Hence, many countries have specific sextortion laws and agencies created to combat sextortion.
6. **Impact on the Victim:** Emotional distress, financial loss, and in some severe instances, complete loss of reputation and career.

The Red Flags of Revenge Porn

Some of the warning signs of revenge porn are as follows:

- Receive comments or indecent remarks from members of some group.
- Receive indecent comments from friends and colleagues
- A failed affair with someone in past.
- Receive threats from an ex-boyfriend for monetary or sexual favors.

The Red Flags of Sextortion

Perpetrators of this offence who carry out this crime have developed their approaches and techniques in order to maximize their chances of success of obtaining the desired result. Some of the common tactics used by these predators to entice victims are as follows:

- Develop a false rapport with the victim
- Record explicit videos and messages during chats secretly
- Use different identities to contact the child
- Pretend to be of the opposite sex or younger to the victim

- Hack accounts in order to steal sexual images
- Threaten to commit suicide if the victim refuses to send sexual images
- Visit public social media profiles to find out more about the victim, including accessing the victim's friend list and searching for other personal information which they can use to cause harm to the victim's reputation.

Suggestions & Conclusion

Technology and the Internet are now an essential part of our lives. This increased reliance on technology and constant engagement with the online world has its both positive and negative repercussions. One's dependency on technology raises extensive challenges in the current scenario. In the negative, it has increased the number of offenders involved in cybercrimes. Without adequate privacy protections, individuals can be subjected to identity theft, data breaches, and other forms of cybercrimes and cyber threats. Digital abuse and cyber threats leading to monetary loss is just one aspect of the challenge. The offence of Revenge porn and sextortion are a violation of the fundamental right privacy and the targeted victim will be left feeling humiliated, angry and depressed. Explicit images which are deeply personal when exposed in the public domain can be emotionally traumatic and have a cascading effect on the victim. Such a violating experience can also have a significant impact on the victim's mental health and wellbeing.

Moreover, the victim feels so ashamed or embarrassed that they are unable to gather the courage to report the crime to the police. However, it is necessary that the victim is reminded that even though they have experienced an instance of revenge porn or sextortion they are not to be blamed, it is in fact the offender who is responsible for the offence.

There is a need for awareness to be created about the offences of revenge porn and sextortion and the abuse and threat that it causes. People must also be made aware that support is available, even if one decides not to report the crime to the police. Following tips can also help to ensure online safety against such digital abuse and cyber threats:

- Avoid accepting a friend request from anyone online if you do not know the person in real life.
- Avoid giving any personal contact info (email or handles) to anyone you haven't met.
- Learn to say NO to those who ask for personally identifying information.
- Do not share your passwords with anyone.
- Keep a password which cannot be guessed easily by reviewing your social media profiles, specially pet names and birth dates.
- Avoid clicking on links in e-mails that come from people who you don't know as doing so would compromise your device.
- Teach teens to report threats. Though they may be stressed or embarrassed, talk freely to them about online safety and encourage them to come forward when they receive any suspicious email or message.
- Be wary of the recording devices bought to keep in homes. Some low-security devices are easy to exploit (like nanny-cams and baby monitors)
- Assume that your webcam or recording devices may be activated remotely. Hence, never keep your phone or other electronic camera devices pointed at you while undressing or when you are in a position that you would not want to share with the world.
- Cover your webcam when you're not using it; if your webcam doesn't have a built-in cover, use a sticker or piece of tape to cover it.

In India, revenge porn is not directly addressed under any law, or defined, and thus it remains a legal grey area. Currently, due to the adoption of the new criminal laws, several provisions of the Bharatiya Nyaya Sanhita (BNS) and the Information Technology Act (IT Act) are being used to deal with revenge porn. Revenge porn is, thus, both a form of sexual harassment as well as an encroachment upon the right to privacy set out in the Information Technology laws.

While there has been much debate over the effectiveness of the current laws to ensure that every woman is provided security across the country, there needs to be a holistic approach to the problems encountered in such regard. There could be two avenues of approach that need to be simultaneously looked like the roots of the problem - awareness and implementation. Raising awareness involves more than mere campaigns and slogans; it needs to be a topic of discourse in public life rather than shunned as a taboo in society. For this purpose, the inclusion of the topic in the school curriculum would go a long way towards sensitizing the future of the nation