Non-consensual intimate imagery: an overview

Rohini Lakshané

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

take back the tech

This publication was developed and produced in collaboration with APC and Take Back the Tech!

Author: Rohini Lakshané

Illustration by Junaid Ahmed Rana

Published by APC 2024

Rohini Lakshané is a feminist interdisciplinary researcher and Wikimedian. An engineer by training, Rohini has worked on several research and advocacy projects at the intersection of technology, policy, and civil liberties. Her body of work encompasses diverse territories such as the application of technology and policy to solve issues of gender inequity and violence; access to knowledge; openness; patent reform; making tech spaces diverse and inclusive; and the cross-hairs of gender, sexuality and the Internet. She enjoys writing and teaching.
https://about.me/rohini

TABLE OF CONTENTS

INTRODUCTION

While the use of digital technologies have been a catalyst for enhancing the freedoms of women and gender-diverse persons, we have also experienced how they can be used as mechanisms for gender-based violence. With the widespread accessibility of smart phones, we have seen an exponential rise in many forms of online violence for more than a decade, one of which has been **non-consensual intimate imagery (NCII).**

NCII refers to intimate photos or videos that are captured, published or distributed without the explicit consent of the person(s) depicted in those images. The meaning and connotations of what constitutes an intimate or sexually explicit image changes vastly with social and cultural norms and contexts in different parts of the world. In this document, we define **intimate images** as sexually explicit, nude or partially nude photos or videos.

NCII are a violation of privacy and of consent, and are a type of **technology-facilitated gender based violence** (TFGBV).[1] When perpetrated by intimate partners, NCII are also a form of **intimate partner violence** (IPV) or domestic violence. NCII impinge on the victim's right to privacy, sexual consent, their freedom of (sexual) expression, and right to live free from violence.

The majority of the victims of NCII are known to be women or gender-diverse persons. However, NCII victims may belong to any gender or sexual orientation.

NCII are symptomatic of the surveillance economy,[2] which threatens the freedom of expression and speech of women, gender-diverse and LGBTQIA+ persons. Personal and identifying details (such as names of the persons in the images) are often attached to the intimate, sexually explicit and nude images being captured or commodified in order to extort, threaten or inflict harm.

---

1 The Association for Progressive Communications has used the term "online gender-based violence" (OGBV) to reflect tech-related violence be it online or off for almost two decades: "Acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email." Association for Progressive Communications (2017), Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences. https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf
Recently, the term tech-facilitated gender-based violence has increased in usage. See more on this reflection in Raghavan, S. (2023, 15 March). Why feminist research is necessary to address technology-facilitated gender-based violence: Recommendations and way forward. GenderIT. https://www.genderit.org/articles/why-feminist-research-necessary-address-technology-facilitated-gender-based-violence
For the purposes of this paper, the terms are considered interchangeable.

2 "...revenge porn is not only an instance of online sexual violence rooted in abjection but also symptomatic of a new political economy of subjectivity, where both the human-based and the automated, algorithm-based circulation of personal information are at the center of processes through which the self is seen and valued, both socially and economically, by others." Langlois, G. & Slane, A. (2017). Economies of reputation: the case of revenge porn, *Communication and Critical/Cultural Studies*, 14(2), 120–138. http://doi.org/10.1080/14791420.2016.1273534

CRIMINALISATION AND THE ISSUE OF "MORALITY"

Sexually explicit, nude or partially nude images may be privately and consensually sent and received between two or more partners as a way of sexual expression and enhancing intimacy. However, in jurisdictions where such activity is deemed illegal, (under, say, anti-obscenity or anti-pornography laws), or "immoral" in the social/public eye, NCII makes those targeted particularly vulnerable to criminalisation, isolation and blame.

LGBTQIA+ persons are especially vulnerable to NCII and its harms in places where being LGBTQIA+ is illegal, is against religious beliefs, or carries social stigma. Known victims of NCII include public figures as much as members of the general public.

When someone experiences an incident of NCII, the reactions from their social circles, families or co-workers, and the discourse in the media may be focused on morality, indecency or impropriety. The victim is blamed for "having brought the incident upon herself" by having shot her own intimate photos or videos, or given access to such images to the person who later non-consensually distributes it, or for having allowed another person to photograph/film her in a sexual act or in the nude. There is often no acknowledgment of the person's consent (or the lack of it) as a determining factor, nor of the prevalence of internet-mediated expressions of intimacy such as "sexting", and coercion within intimate relationships.

Restricting NCII to a matter of morality glosses over the realities of violation of consent, breach of privacy, IPV/TFGBV, and the far-reaching impact on the life and wellbeing of the victim. As access to smartphones, inexpensive spy cameras and the internet grows, so does the number of NCII cases worldwide. Global responses rooted in local experience are vital.

Women and gender-diverse persons finding, establishing and navigating love, sex, intimacy and relationships online often walk a razor's edge between risking harm and experiencing mutually rewarding sexual interactions. Online sexual expression is an act of reclaiming digital technologies for our pleasure, creativity and agency, and can enhance our enjoyment of and power in intimate relationships. This paper aims to present a global South perspective on the risks that NCII poses, and propose strategies for responding to and safeguarding oneself against NCII incidents.

DEFINITIONS AND THE PROBLEM WITH THE TERM "REVENGE PORN"

Other terms used to describe NCII are "image-based sexual abuse" (IBSA), "non-consensual pornography" (NCP), "non-consensual sharing of intimate images" (NCSII), and "revenge porn". On the websites and platforms that distribute NCII, it may be described as "revenge porn", "amateur porn", "hidden cam porn", or "sex scandal". In languages other than English, it goes by local names, such as "molka porn" in Korea, *molrae-kamera* being the Korean word for concealed cameras intended to record voyeuristic content. In India "MMS" and "MMS scandal" are terms used to describe surreptitiously shot and/or leaked videos as a reference to the Multimedia Messaging Service format in which digital NCII was circulated in its early years in India.

Other definitions: According to Burris, "At its core, nonconsensual pornography is involuntary pornography… The primary issue with revenge porn is consent: someone publically distributes the sexually graphic images of others without their consent."[3] Franks provides a succinct definition of revenge porn in her guide for legislators, simply stating that "nonconsensual pornography refers to sexually explicit images disclosed without consent and for no legitimate purpose."[4]

However, referring to NCII as any form of "porn" is inaccurate and can be harmful. Pornography is a consensual form of expression and labour;[5] NCII is a non-consensual act intended to harm and disempower those targeted.

Why the term "revenge porn" is harmful

The term "revenge porn" is commonly used to describe NCII inflicted by the victim's former sexual partner. However, the term misidentifies and conflates pornography - a consensual act - with what constitutes a breach of privacy and an act of violence. Using the term also implicitly affirms

- The non-consensual capturing, publication or distribution of intimate images is a reaction or an act of retribution against real or perceived wrongdoing committed by the victim and that the victim deserves blame for the vengeful act.
- Capturing one's own intimate images, even with the expectation that the images will remain private, is a pornographic act and the person doing so is making pornography; that images of sexual expression showing nudity or sexual activity are inherently pornographic.[6]

In addition to such erroneous assumptions, the term also glosses over the fact that NCII are a systemic and societal problem and a flourishing and lucrative industry, not solely a matter of personal vendetta. Revenge porn is differentiated from other NCII by the motive of the person who started their distribution. However, there are several entities in the "supply chain" of NCII, so to speak, that enable or facilitate its creation and perpetuation. Some of these entities are discussed in subsequent sections of this paper.

Also see: "Revenge Porn": 5 important reasons why we should not call it by that name.

3 Burrus, A (2015). Hell hath no fury like a woman porned: Revenge porn and the need for a federal nonconsensual pornography statute. Florida Law Review. 66(6). https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1789&context=flr

4 Franks, M.A. (2015) Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators. *Social Sciences Research Network*. https://ssrn.com/abstract=2468823

5 "We recognise that the issue of pornography online has to do with agency, consent, power and labour…We support reclaiming and creating alternative erotic content that resists the mainstream patriarchal gaze and locates women and queer persons' desires at the centre." Feminist Principles of the Internet. (2014). Pornography. https://feministinternet.org/en/principle/pornography

6 In some countries anti-pornography laws are so restrictive they may consider consensual capture of intimate, nude or sexually explicit images as an act of producing pornography, even when the images are expected to remain private; Franks, M. A. (2017) "Revenge Porn" Reform: A View from the Front Lines. Florida Law Review, 69(5). https://scholarship.law.ufl.edu/flr/vol69/iss5/2

TYPES OF NCII CONTENT

The capturing and/or sharing of sexually explicit or nude images can constitute a case of NCII when there is non-consensual *capture* of those images, non-consensual *distribution* of those images, or both. It can also include manipulated images. This section outlines different types of violations of consent and who is likely to inflict them.

NCII capture and distribution, as well as image manipulation, are typically performed by perpetrators whose motives may be:

- Discrediting, slut-shaming, publicly shaming or defaming the person(s) in the NCII, thus causing them humiliation, distress and harm.
- Discrediting or defaming a political or public figure or person in active public life by creating the public perception that they are morally corrupt and/ or promiscuous.
- Revenge for rejection of their sexual or romantic advances.
- Revenge for the NCII victim's real or perceived wrongdoing that does not involve interactions of a sexual or romantic nature (for example, a personal quarrel or a hostile former friend)
- Sextortion: coercing the victim into performing or participating in sexual acts or providing more sexual imagery.
- Exposing the identity of LGBTQIA+ persons where these sexual identities/orientations are illegal or social or religious taboo.
- Monetary gains, for example:
  - Extortion from victims by telling them to pay money in return for not publishing the NCII or taking down NCII from a site where they have already been published (also considered sextortion).
  - Selling the NCII to pornographic websites, other adult content services, or offline distributors of pornographic content.
  - Advertising or subscription revenues earned from pornographic websites or file-sharing services
- Non-monetary gains such as gaining reputation and credibility in an online or offline community, obtaining validation from the community, or self-gratification.
- Storing the images non-consensually for private use, without the intent to distribute them to other people.

Voided consensual capture

In cases where a person is aware of the presence of a camera and consents to their intimate images being captured, consent may be legally considered void in the event that the consent is:

- Obtained via coercion
- Of an inebriated person (under the influence of alcohol or drugs).
- Of an underage person
- Of a person with severe mental illness
- Of a severely intellectually disabled person

In these cases, the images or videos recorded may be considered NCII.

Non-consensual capture

A. Clandestinely captured images

Non-consensual capture occurs when images are shot surreptitiously via hidden cameras planted in places where a person would generally and reasonably have an expectation of privacy, such as a bathroom. The person(s) in the frame in such images are not aware of the presence of the camera. This is typically done by:

- Owners or staff working in hotel rooms or rented accommodation (such as AirBnB), spas, massage centres, changing rooms at swimming pools or gyms, changing rooms at clothing stores, or restrooms in public places or in restaurants and pubs.
- Voyeurs
- Cyberstalkers/physical stalkers (via hidden cameras and/or spyware)
- Sexual or romantic partners of the person(s) in the NCII. Typically, this case occurs when the person in the frame in the NCII refuses to share nude/semi-nude selfies or make sexually explicit videos for their partner, and as a result, the partner who is denied consensual access resorts to clandestinely shooting the images without appearing in the frame. Either that or the partner suspects the person in the frame of infidelity and wants proof of their intimate acts. This may be done via concealed cameras or the use of spouseware, a type of commercial spyware that spies on the device on which it is installed.
- Individuals whose romantic and/or sexual advances have previously been rejected by the person(s) in the NCII.
- Clients who surreptitiously record interactions on paid adult webcam services such as Chaturbate.
- Someone with vendetta who is not a current or former intimate partner.

B. Images captured with the knowledge of at least one of the persons in the frame

At least one person in the frame is aware of the presence of the camera and the fact that it is switched on. Typically, the camera is set up by a sexual partner before a sexual act, without the knowledge of the other person(s) in the act. It is possible that the perpetrator of the NCII may be in the frame.

Consensual capture but non-consensual distribution of images

This is typically the case when:

- An individual, couple or more persons consensually shoot their intimate or sexual acts on video for private use.
- An individual takes sexually explicit/nude photos (sometimes referred to as naked selfies; or "nudies").

There is one or more persons in the frame and each one is aware of the presence of the camera and the fact that it is switched on, and they consent to their sexually explicit images being captured.

The individuals in the photos or videos may stream or send them privately and consensually to one or more intimate partners via online or offline means. However, they do not expressly consent to the publishing or distribution of the images online or offline to anyone other than the intended recipients. Non-consensual distribution may happen in four scenarios:

- One of the intimate partners publishes/distributes the images without consent.
- One of the intimate partners threatens to publish/distribute the images.
- Someone who has obtained access to the images without the consent of the persons in the frame (for example, a malicious hacker or a colleague) further distributes the images without their consent.
- The intended recipient of consensually shot images is not a sexual or romantic partner but a client paying for the images which are meant for private use (for example, when subscribers of sexual content services such as OnlyFans access images for their private use). The client records/stores the images and distributes them without consent and in violation of the terms of the service.

One example of the non-consensual distribution of consensually captured videos are the multiple incidents of videos being clipped from surveillance footage of the Delhi Metro showing couples getting intimate in empty carriages, which were leaked on porn websites. Everyone boarding the train is made aware of the presence of surveillance cameras through audio announcements and visual signage, so the couples were aware they were being recorded. However, surveillance footage of a public transport service is expected to be highly secured and guarded, and it is unlikely that anyone would reasonably expect it to be distributed on the public internet, even less so as pornography. In one of the incidents, the metro company filed a police complaint against the couple in the video on grounds of obscenity in a public place but did not make any public statement about taking action against the person(s) who may have leaked the footage.

Non-consensual access and distribution of images

Non-consensual distribution may happen when:

A. Malicious actors consensually capture images as described above and distribute them.

B. Malicious actors who did not capture the images but are known to the victim gain access to the images via the devices and/ or accounts of the victim. In particular, a person can be vulnerable to NCII in instances where they share living or working spaces with others and their phone or laptop are easy to physically access. A person's vulnerability also increases when they have online accounts for which they share login details with other people.

C. Malicious actors who did not capture the images and are not known to the victim(s): The motive may be financial gain, extortion, voyeurism, political benefits, a feeling of religious or moral righteousness (in a case where the victim is viewed as being anti-religious, irreligious or morally corrupt or of bad character), or to seek self-gratification or validation online. As long as such actors can access a person's devices or accounts where images are stored, that person is vulnerable to NCII. The instances may include:

- Unauthorised access of a victim's device or online accounts by unethical hackers who seek to "leak" the images for monetary or non-monetary gains. Public figures in particular are often targeted.
- When a person sends their device for repair, technicians may decide to scan the device for the potential presence of sexually explicit content, and may be able to recover even deleted images through data recovery tools.
- When a person sells or discards their used/ defunct device, persons who deal in these devices, scan them for sexually explicit content. They may be able to recover even deleted images via data recovery tools.
- Hotel rooms or rented accommodation (such as AirBnB rooms), spas, massage parlours, changing rooms at swimming pools or gyms, trial rooms at clothing stores, or bathrooms in public places or in restaurants and pubs where NCII are surreptitiously captured and further distributed.
- Non-consensual pornographic deepfakes or other kinds of manipulated sexually explicit imagery.
- Exposé groups, "activists" and vigilante groups whose self-declared aim is to expose what they consider is [the victim's] moral corruption, misconduct, bad character or deviation from the rules of their religion. These elements may carry out incidents of NCII and term it as delivering "justice".

Manipulated images and disinformation

NCII can consist of a real image of a person that is digitally manipulated to make the person look nude or in a sexually explicit act. Typical examples include images in which:

- A person's face is superimposed on a nude/sexually explicit image of another person.
- A person's real photograph is altered to show naked genitalia or full or partial nudity.
- Deepfake images or videos. Deepfakes are created using artificial intelligence (deep learning, hence the name) to create convincing fake images which depict a person saying or doing something they did not. Sexually explicit deepfakes usually require sophisticated technology and training to create, and often target public figures, but as the technology becomes more accessible, cheaper and easier to use, they may be increasingly used to target anyone.

The manipulated images may be accompanied by identifying details such as the victim's name.

While the image may not be completely that of the victim and the deepfake image is not that of a "real" act or person, the negative impacts on the victims and the intent of the perpetrators are the same as other kinds of NCII.

Another instance is the use of altered or misleading images with accompanying mis/disinformation, which are used to target the victim. For example, a fake nude photo of German politician Annalena Baerbock that appeared on the internet in 2021 was that of a Russian porn star with a vague resemblance to her.

MODES OF DISTRIBUTION OF NCII

"Downstream distribution" is a term used to describe the reposting of NCII done by entities that did not capture or create the NCII and did not originally post it on the internet or start its offline distribution. These entities enable the endless perpetuation of NCII even when it's removed from its original source on the internet, making it nearly impossible to permanently remove the NCII from the internet.

NCII distribution happens via both online and offline streams listed below, which perpetually feed into each other. For example, it may originate from one source, say, a camera planted in a hotel room, then be uploaded on a pornographic website, from where someone downloads it and further distributes it via a channel on the Telegram messaging app, from where someone else downloads it and transfers it to a USB drive or memory card, which is then used to distribute the NCII further. The different entities involved in the "supply chain" may or may not know each other or act in coordination with each other.

Online vehicles of distribution can include:

- Pornographic websites, especially those that do not verify age or consent of the person(s) in the images. Some sites exclusively post NCII.
- Exposé groups and broadcast channels on messaging applications such as WhatsApp and Telegram, on social networking services, and messaging boards such as 4Chan and 8kun.
- Peer-to-peer file distribution services, file-sharing and transfer services (For example, torrents, Dropbox and EasyShare)
- Image-sharing websites, some of which are meant solely for distributing sexually explicit images (for example, the now-defunct Nangaspace.com)
- Extortion and defamation websites created solely for the purpose of publishing NCII, often along with identifying information of the victims. (For example, Is Anyone Up?, MyEx.com, and YouGotPosted.com, all three of which are now defunct.)
- Dark web: The dark web is hidden by its very nature, difficult to regulate, not searchable via search engines and requires the use of a special browser.
- Social media, although most of the major social networking services do not accept sexually explicit content and have policies against posting NCII.

Offline means such as:

- DVDs or Blu-Ray discs sold via clandestine channels.
- Memory cards or USB drives containing NCII content. The cards/USB drives are sideloaded on mobile phones or other devices and/or copy-pasted into more cards and drives in the distribution chain.

ILLUSTRATIVE INSTANCES OF NCII

- Is Anyone Up was an NCII website started by Hunter Moore in the US that ran from the year 2010 to 2012. The images on the website were juxtaposed with personal information such as the names, home addresses, contact information and the social media identity of the victims. The images were submitted anonymously and non-consensually by former partners of the victims and were not taken down even when the victims requested so. Moore also paid a hacker to break into email accounts and obtain sexually explicit photos to post them on the site. The website urged viewers to write disparaging comments on the photos.

- Incident in Karavali, India, 2010-2011. The victim was a university student who ended her relationship with her boyfriend. As a vindictive act, he published their intimate photos and videos on the internet without her consent. She filed a police complaint against the former boyfriend, who was subsequently charged. The incident was reported in the media by the names "Karavali Sex Scandal" and "Karavali MMS Scandal". Later, an employer withdrew its employment offer to her after her police complaint came to light in an antecedent check. The employer was the Intelligence Bureau (IB), an internal intelligence agency of the Indian government. According to news reports, the agency stated that she had been rejected on grounds of her "questionable conduct" and "calibre".

- Ugandan model Judith Heard received an email in 2013 threatening her to pay $3,000 in lieu of not publishing her nude selfies on the internet. She did not pay, after which the photos appeared online without her consent. In 2018, her nude photos were leaked again and she was arrested under Uganda's anti-pornography law. She has stated that she did not send the nude photos to anyone and that she believes the photos were stolen from her phone.

- Hidden cameras in motels in South Korea, 2019. Two men planted hidden cameras in 30 motels across 10 cities in South Korea and streamed the videos of the intimate acts of the occupants online for financial gains. The police stated that the cameras were hidden in hair dryer holders, satellite boxes and closed electrical sockets. South Korea has a high incidence of spy-camera pornography.

- Hidden cameras in AirBnb houses. There have been instances of Airbnb users detecting hidden cameras in places they have rented via the site. AirBnB has a policy against planting "concealed and undisclosed devices" and those "located in or monitoring private spaces." AirBnB also requires that its users "always disclose if an active recording is taking place." In the event that AirBnB users need help, the policy states they "first contact local law enforcement authorities for assistance" and contact AirBnB about the violation of its policies.

REPERCUSSIONS FOR VICTIMS

Victims often learn about the incident(s) of NCII after their images appear online or when they are being threatened that their NCII will be posted or circulated online.

Victims whose images are published and distributed without their consent via online and offline means face a range of repercussions:

- Stalking and physical harm
- Defamation
- Extortion from the victim or their family
- Cyberbullying
- Loss of employment or professionally-held positions/loss of employment opportunities
- Expulsion from school/university or other kinds of loss of educational opportunities
- Eviction from rented homes
- Being denied rented accommodation by homeowners
- Disownment by family and/ or eviction from the family home
- Social ostracism
- Coercion and threats (of death, rape, etc)
- Harassment (online, offline or both)
- Forced displacement (having to flee to another state, city or country as a direct or indirect consequence)
- Physical, emotional and psychological harm and distress
- Criminalisation and arrest
- Secondary repercussions such as financial distress caused by loss of employment/ income, and negative impacts on the victim's family in places where notions of "family honour" exist and are tied to moralistic ideas of the chastity of women/ gender-diverse persons.
- Some victims attempt suicide.

RISKS

- Shooting one's own intimate images, even when done privately and consensually, is frequently considered unacceptable by social norms, religious beliefs or moral codes in most places. When an NCII incident occurs, religious groups or individuals with a vigilante sense of protecting public and private morality may blame, harass, defame or otherwise try to harm the victim. They view the consensual shooting/sharing of intimate images as damage to public morality, as an act of obscenity/indecency or pornography, and as an encouragement to women to shoot and distribute their own sexually explicit images. In cases where the NCII involves persons not married to each other, they also view it as a violation of the social and religious diktats against sex before or outside marriage.

- Legal or judicial remedies may be inadequate or non-existent
  - Some places do not have legislation or legal instruments to adequately address NCII.
  - In places where laws against obscenity and/or pornography do not acknowledge the private and consensual nature of intimate images, victims tend to be criminalised for "making pornography" or for obscenity.
  - The law needs to recognise that (a) the consent of the subject(s) of the intimate images is a deciding factor while differentiating NCII from pornography and from the freedom of (sexual) expression; (b) the right to privacy is inalienable, that is, one cannot give up the right even if one does not want it.

- Sexual and/or privacy rights do not enjoy strong protections in some places.

- When minor individuals consensually and privately capture such images of themselves or other minors, it may amount to child sexual exploitation according to the law in some places.

- NCII are known to be rapidly and virulently distributed on pornographic websites, peer-to-peer file-sharing services, instant messaging applications, messaging boards, social media, sites on the dark web, among other online platforms. The expansive capacity for the internet to replicate data[7] and the inexpensive and easy accessibility and affordability of certain software tools and online services facilitate the quick redistribution of NCII from the source and also ensure that the content remains in circulation almost indefinitely. NCII have an indelible digital footprint, if not permanence.

- The easy and quick discoverability and searchability of NCII increases the distress of the victim, while providing the perpetrator(s) validation, avengement, or monetary benefit. The cost to the victim increases in places where NCII is a flourishing and lucrative industry and/or where there are desirable social gains from perpetrating NCII.

- Users of pornographic websites, adult messaging boards, and social media websites make attempts to identify the person(s) in NCII via the comments or messaging sections. They may be able to establish the real life identity of the persons in NCII, including details such as their place of work or

7 This happens via automated means or manual ones or a combination of both. The processes include but are not limited to scraping; mirroring; torrenting; the use of social media bots/pages/accounts; and automated and manual sharing on instant messaging (IM) applications (Channels on Telegram, for instance).

residence, which may have repercussions for NCII victims. Even when they are unable to correctly establish the identity of the NCII victim(s), there is a risk of mistakenly identifying an unrelated person who may then face the same repercussions.

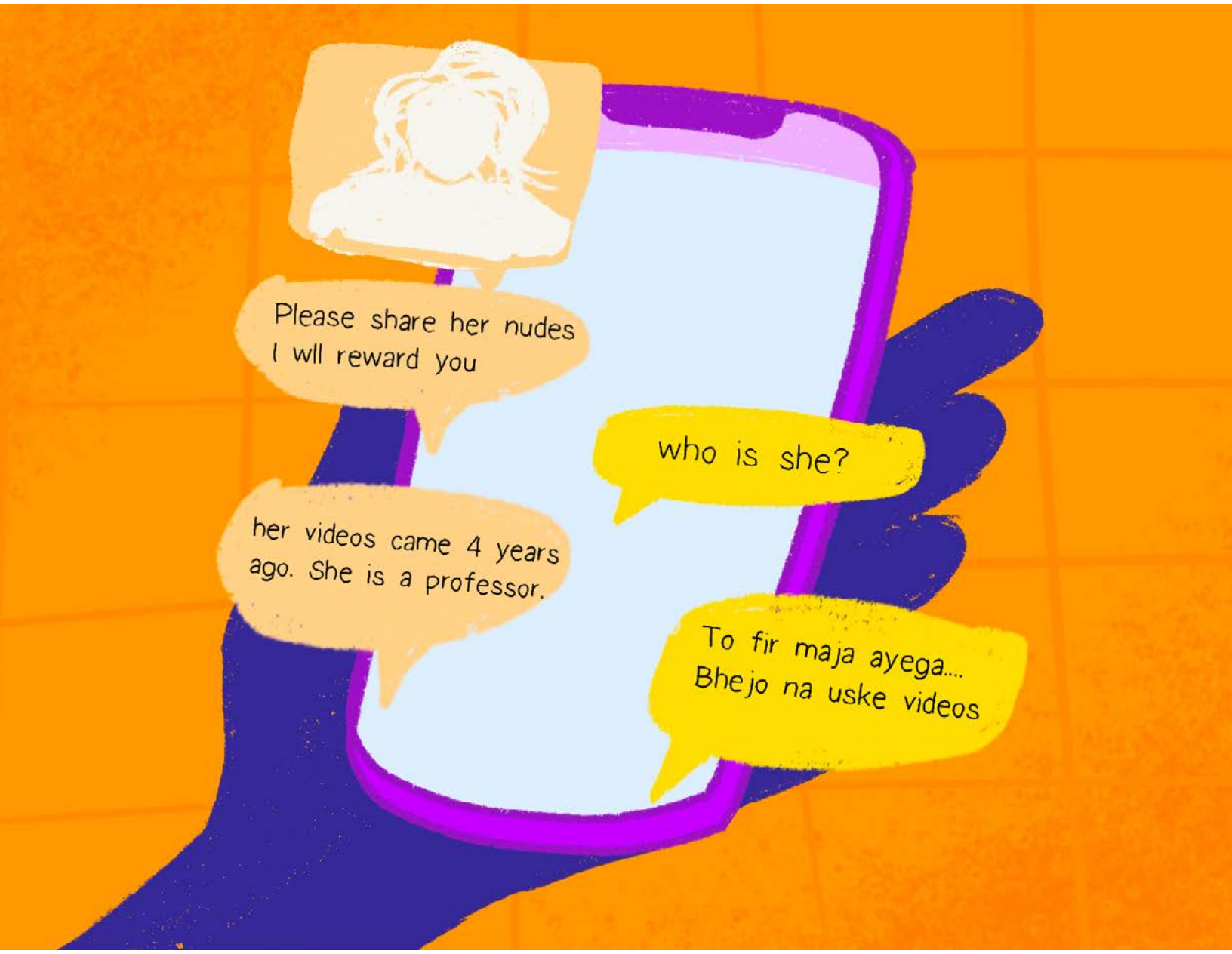

Illustration of a real example of online exchange “Please I need her nude pics and vids” to obtain personal information linked to an instance of NCII. The link to the specific example is removed for ethical reasons, but the conversation finalised in provision of the actual video link requested. Inside the secret world of trading nudes examines similar efforts to doxx NCII victims.

RIGHTS

Right to privacy

NCII is a violation of the right to privacy when the images are intended for private use and there is no explicit consent for their distribution (such as a voice recording, signed consent form or media release). It is also a violation of privacy in instances where the images have been shot clandestinely in a place or setting where there is an expectation of privacy.

Freedom of (sexual) expression

It is easy for NCII to be conflated with pornography or free and consensual capture and distribution of sexual expression. The key difference between NCII and sexual expression is the explicit consent of the person(s) in the image or video to have their image captured or distributed.

Right to live free from violence

NCII are an act of many types of violence: sexual violence and abuse; technology-facilitated violence; intimate partner violence when perpetrated by a current or former partner; gender-based violence when targeted at women and gender-diverse persons; and emotional and psychological violence against the victim. NCII may also result in physical violence, for example, stalking, arrest or physical assault on the victim. The repercussions on victims also tend to be far-reaching and almost indefinite. Thus, NCII are a violation of the right to live free of violence.

Right to live with human dignity

Every person has a right to live a life that is dignified and free of discrimination in which the person can claim respect from other persons and the state. Some of the repercussions of NCII discussed above violate this right.

Right to be forgotten

This right can be invoked to have the private information and images of the victim removed from internet search engines.

Right to justice

The right applies in the case of victims who initiate a judicial process. The right guarantees the protection of the law to everyone and the ability to seek legal remedies.

Consumer rights

Based on the jurisdiction, it may be possible to file a complaint of the violation of consumer privacy or other consumer rights in cases where a company posts an NCII and does not take it down despite a request.

Copyright

Copyright is a type of intellectual property and protects the rights of the creator of an original work. Copyright is applicable to works of sexual expression and can be applied in cases such as work that is positioned as pornography. Similarly, copyright can be used to take down NCII. Sex workers who make their sexually explicit images and videos available for a fee, for example, via services such as OnlyFans or Chaturbate, may invoke copyright in case the clients/subscribers distribute their images without their permission and consent.

STRATEGIES

Victims of NCII need support for their mental health, legal processes, physical and/or digital security and financial needs, among other things. While laws and judicial mechanisms to address NCII exist in some jurisdictions, victims may hesitate to seek help, may be unaware of the legal/non-legal recourse available to them, and have little access to social, legal or mental health support. Deeply entrenched patriarchal notions of honour and shame remain attached to the bodies of women, gender-diverse persons and LGBTQIA+ persons. Social conditioning disfavours the victim because the consent of a woman, gender-diverse or LGBTQIA+ person is not recognised as a legitimate factor in determining moral standards. Victims hesitate to seek help or justice on account of stigma, humiliation, the possibility of being victimised in additional ways, and processes that may be prohibitively challenging, long, protracted and expensive. In that sense, the process to obtain a remedy is often as much a punishment as the distress of the NCII incident itself.

Practising good digital and physical security

One of the ways to prevent persons other than the intended recipients from getting access to NCII in the first place is to practise good digital security such as safe sexting and safe storage of sexually explicit images. Implementing certain kinds of security checks and precautions does reduce the spontaneity of sexual interactions online and in the physical world. It also requires that one or more partners learn the skills to properly implement these measures and that everyone involved understands and appreciates the need for safe sexting/physical security checks. Thus, it is best to have a conversation with the partner(s) beforehand about physical and digital security, so that sexual interactions continue to be safe, non-coercive and pleasurable.

Resources on good digital security practises for sexting and storage of sexually explicit images:

- The Motherboard Guide to Sexting Securely https://vice.com/en_us/article/mb3nd4/how-to-sext-securely-safely-what-apps-to-use-sexting
- Hack Blossom https://web.archive.org/web/20180602215706/https://hackblossom.org/domestic-violence/threats/sexual-content.html
- Hey Friend from Take Back the Tech https://takebackthetech.net/know-more/heyfriend
- How to take private photos on Signal https://freedom.press/training/taking-private-photos-signal
- Safer Nudes (including printable zine) https://codingrights.org/en/project-item/safer-nudes-2/
- Safer Sisters Online Security Tips in GIFs https://medium.com/codingrights/safersisters-online-security-tips-in-gifs-222589166ed8
- For teens from Planned Parenthood
  https://plannedparenthood.org/learn/teens/bullying-safety-privacy/all-about-sexting
  https://plannedparenthood.org/learn/teens/bullying-safety-privacy/online-privacy-and-staying-safe
- How to find a hidden camera in an Airbnb (video) https://www.youtube.com/watch?v=N88G1Pp8Qvs
- How to find hidden cameras in an Airbnb or in a hotel https://www.tiktok.com/@malwaretech/video/7002804220126661893
- Does your Airbnb or hotel have a hidden camera? Experts share tips for protecting yourself. https://www.washingtonpost.com/travel/tips/airbnb-hidden-camera-tiktok

- Holistic security strategies and measures to address non-consensual intimate images (NCII) https://wougnet.org/holistic-security-strategies-and-measures-to-address-non-consensual-intimate-images-ncii

Other precautionary tips

There are certain practices that, when integrated into your everyday use of digital devices, can greatly enhance the safeguarding against and prevention of NCII. These include:

- Cover in-built phone and laptop cameras with a removable sticker.
- Cover or remove web cameras from desktops.
- Use an EXIF data removing tool to delete metadata from sensitive photos before sharing them. For example, the open-source ScrambledEXIF app for Android allows removal of metadata in bulk.
- Similarly, remove metadata from sensitive videos.
- At a hotel, AirBnb accommodation or similar places, inspect the room to check if something looks out of place, like a slightly misfit tile in a faux ceiling.
- Never leave mobile phones, laptops or other personal devices unattended and be careful about giving physical access to your devices to anyone, even if intimate images or videos have been deleted from them.
- Consider using ephemeral messaging services instead of using the private messaging feature on social media websites for the purpose of having intimate conversations.
- Check your privacy settings on social media accounts and make sure they are the visibility level at which you are comfortable.
- Consider not using free-of-cost virtual private networks (VPNs) because most of them are unsecured and are used to mine the data and personal information of the users.
- Be wary of persons you meet on dating apps and similar services who ask for nude/sexually explicit images, especially when your acquaintance is very new.
- Change your device's name in the settings e.g. from "Andy's computer" to a name that is not personally identifiable, e.g. "Doraemon".
- Consider using anti-virus software that detects and flags spouseware or stalkerware.

Self-doxxing

Doxxing involves searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent. Self-doxxing may be practised as a precautionary measure or while facing an incident of NCII to discover the places where NCII have been uploaded.

Google Alerts

Set up Google Alerts for your full name, prior names, home addresses, email addresses, phone numbers, social media handles, and other personal information. Include text, images and video alerts.

Reverse image search

As a precautionary measure, use the Reverse Image Search function on Google Images and TinyEye to search for unauthorised publishing of your photos such as those posted on your social media accounts or on dating apps.

In case an incident of NCII has occurred and you are aware of it, then reverse image search will enable you to discover pornographic websites, messaging boards and other platforms where the NCII have been posted.

Preemptively submit one's own intimate images and videos

StopNCII.org, a free global platform enables users to pre-emptively request takedown of their own intimate images in case they fear that the images will be uploaded without their consent to any of the initiative's member platforms. Members of the StopNCII initiative include the dating app Bumble, the video-hosting service PornHub, TikTok, Facebook, and Instagram, among others. The submitted images never leave one's personal device and are not stored online at StopNCII.org. Instead, a fingerprint of the photo is generated on the user's device, creating a unique identifier of the photo known as a "hash", which is then uploaded and stored in the bank of fingerprints. StopNCII.org partners then eliminate the photo identified by the hash from their platforms.

Facebook, Twitter and Google have also been using a tool named PhotoDNA to detect images that constitute child sexual exploitation/child pornography since 2011.

Content deletion and reputation management services

There are paid services that search for public records online in real time and enable their users to manage their presence on the internet. Such services should be used with discretion and examining customer feedback. While this paper does not recommend any specific service, examples include DeleteMe and Internet Removals.

Legal remedies

Some jurisdictions have passed laws against NCII, such as Europe, the UK, the US, Australia, Canada, Philippines, Israel and Japan.[9] There is current and proposed legislation in response to NCII in Kenya, Chile and South Africa.[10]

Typically, other laws applicable would be those dealing with:

- Privacy
- Cybercrime

8 The Centre for Internet and Society. (2018). Revenge Porn Laws across the World. https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world

9 Centre for International Governance Innovation. (2021). Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa. https://www.cigionline.org/static/documents/SaferInternet_Paper_no_2_SuBHPxy.pdf

- Cyberbullying
- Defamation/libel
- Data protection
- Unlawful surveillance
- Copyright infringement
- Laws addressing violence against women, including those against domestic violence and intimate partner violence
- Cyberstalking/stalking
- Extortion
- Illegal hacking/cracking
- Sexual assault (in case of images or video of sexual assault or rape being circulated online)
- Child sexual exploitation/child pornography (if the victim was underage at the time the image was captured)
- Intimidation/ severe harassment.

A copyright infringement claim may be filed, especially in the case of selfies or self-shot videos, that is, the person taking the sexually explicit selfie or video is its rightful copyright holder who may demand that the website/service stop unauthorised publishing and distribution of the photo or video and possibly even compensate the owner for infringement.

However, legal responses are not consistently enshrined around the world and are often poorly enforced. In places where it is illegal to be LGBTQIA+, legal remedies for NCII incidents are not accessible to LGBTQIA+ persons.

A. Legal notices for removal of images and videos

The victim or their representative may send a legal request to websites or file-sharing services telling them to completely and permanently remove the NCII content from their respective servers and content management systems,and, where possible, prevent the upload of the same content again. Whether or not these services honour the request depends on a number of factors, including local laws, the safe harbour these services have (for example, under intermediary liability laws and regulations), and their own policies/terms of service (ToS) regarding non-consensual content, privacy, copyright and pornography. File-sharing and encrypted cloud storage services usually disclaim any responsibility for the content uploaded on them and state that they act only when they receive a legal notice or someone files a report of alleged violation of their ToS.

B. File a police report

Filing a police report may be challenging because police personnel may not be adequately prepared, trained or sensitised for handling NCII incidents. They may believe that victims are to blame or that content on the internet cannot be controlled. They may also lack institutional capacity, that is, lack the tools, skills and knowledge necessary to respond to complaints involving NCII or to counter the actions of perpetrators who distribute NCII. Some towns and rural areas usually do not have a cyber

department of law enforcement, which prevents the victims from taking the basic step of lodging a police report even when they want to do so. However, it may be unavoidable considering that some types of legal responses require that a police report be filed as a first step. Secondly, it may be in the interest of the victim to have an official, documented record of the incident.[10]

C. Judicial orders to web search engines

Depending on local laws, it may be possible for victims to obtain an order from a court of law directing search engines to de-index NCII content, and directing other services (for example, cloud storage andpornographic websites) to takedown NCII content. While de-indexing does not remove the NCII content from the internet, it drastically reduces its discoverability via search engines, and thus reduces access to the content and its subsequent distribution.

Takedown requests to platforms

Many internet companies have policies against NCII and have a defined process for victims to make a content removal request as well as to report a violation of the NCII policy. However, platforms tend to fail to enforce their own takedown policies, and when such takedowns do happen, the process may not be swift.

A document entitled "Resources on Non-Consensual Distribution Of Sexually Intimate Images" issued by the California government states the image removal policies and remedial information for the following services:

- Facebook
- Google
- Microsoft
- Google
- Tumblr
- Twitter
- Yahoo

A related page contains a compilation of links on image removal policies and remedial information for other popular sites:

- 4Chan
- About.me
- Ask
- AOL
- Flickr
- Lycos
- MySpace
- Snapchat

10 For advice (albeit US-centric) on documentation of the NCII incident itself: Cyber Civil Rights Initiative. CCRI Safety Center. https://cybercivilrights.org/ccri-safety-center#document

Additional online resources for image take down requests on different platforms:

- Image removal from **Reddit** (guide created by the Cyber Civil Rights Initiative): https://perma.cc/7RQ6-LJZL
- **PornHub**'s non-consensual content policy, which includes information about reporting a violation and requesting removal of content https://help.pornhub.com/hc/en-us/articles/4419871787027-Non-Consensual-Content-Policy
- How to remove non-consensual videos from PornHub https://www.vice.com/en/article/epgpqa/how-to-remove-videos-from-pornhub
- **Imgur** removal request page https://imgur.com/removalrequest and an accompanying help page https://help.imgur.com/hc/en-us/articles/210080953-Deleting-Posts-and-Images
- **Photobucket**'s policy for removal of "personal images posted without permission" https://support.photobucket.com/hc/en-us/articles/4402291602068-Personal-Images-Posted-Without-Permission
- English **Wikipedia**'s "Guide to image deletion", which addresses instances of copyright infringement https://en.wikipedia.org/wiki/Wikipedia:Guide_to_image_deletion
- English **Wikipedia'**s image use policy. https://en.wikipedia.org/wiki/Wikipedia:Image_use_policy (See the sections on "privacy rights" and "legal issues".)

RESOURCES

Acoso.online
https://acoso.online Resources for NCII victims living in 17 countries in Latin America as well as Spain. (Website in Spanish; some pages exist in English)

Dirty Code
https://dirtycode.io An alternative to sending actual nude images. It generates an illustration of genitalia based on the user's specification of its size, colour etc.

A personal story: Love in the time of cryptography
https://wired.com/2017/04/love-in-the-time-of-cryptography A personal reflection on the lack of digital footprints in a present-day romantic relationship.

End Cyber Abuse
https://endcyberabuse.org A global collective of lawyers and human rights activists working to tackle NCII. Among other things, it has published "Orbits: a global field guide to advance intersectional, survivor-centred and trauma-informed interventions to TGBV" https://endcyberabuse.org/orbits

Revenge Porn Helpline
https://revengepornhelpline.org.uk Helpline for adult victims who live in the UK.

Cyber Civil Rights Initiative https://cybercivilrights.org A non-profit organisation in the US that provides services to NCII victims, among other things. The founder was a victim of NCII herself.

Without My Consent is a non-profit organisation in the US that is now a project stewarded by the Cyber Civil Rights Initiative. Its website contains useful resources for victims https://withoutmyconsent.org/resources

Resources for victims who live in the state of California in the US
https://oag.ca.gov/cyberexploitation Content removal process under the Digital Millennium Copyright Act in the state, refer to https://oag.ca.gov/cyberexploitation/victims (specifically, #9. What should I do if I have experienced cyber exploitation?)

What To Do if You're the Target of Revenge Porn
https://consumer.ftc.gov/articles/what-do-if-youre-target-revenge-porn Guidance issued by the US Federal Trade Commission.

Tips to prevent instances of NCII as well as to remedial steps to take in case an incident occurs, by the **Cyber Crime Support Network**, a non-profit organistion in the US https://fightcybercrime.org/scams/harassment/revenge-porn (Archive link: https://web.archive.org/web/20220708132008/https://fightcybercrime.org/scams/harassment/revenge-porn/)

Articles containing guidance in the Indian context

- What to do if you are a victim of revenge porn https://blog.ipleaders.in/victim-revenge-porn
- Ways to prevent revenge porn incidents https://blog.ipleaders.in/ways-prevent-revenge-porn-incidents
- Here's what you need to do if you end up being a victim of revenge porn https://blog.ipleaders.in/heres-what-you-need-to-do-if-you-end-up-being-a-victim-of-revenge-porn
- How to file a police complaint in India https://pinklegal.in/topics/police/police-complaint.html
- Peeping Tom Porn and Privacy https://genderit.org/feminist-talk/peeping-tom-porn-and-privacy

Need Help Now

https://needhelpnow.ca/app/en Resources for NCII victims living in Canada.

Articles containing guidance from a UK context

- Dealing with content for ransom
  https://www.thecyberhelpline.com/guides/content-for-ransom
- Dealing with webcam blackmail (sextortion)
  https://www.thecyberhelpline.com/guides/webcam-blackmail
- Guide on steps to take for digital safety after ending a relationship
  https://refugetechsafety.org/digitalbreakup

Resources for young persons in Australia

- Non-consensual sharing of nudes
  https://www.esafety.gov.au/young-people/my-nudes-have-been-shared
- Someone threatening to share nudes
  https://www.esafety.gov.au/young-people/someone-threatening-to-share-my-nudes
- Being pressured into sharing nudes
  https://www.esafety.gov.au/young-people/being-pressured-to-send-nudes

Articles containing guidance from an African Context

- Gender, law and revenge porn in sub-Saharan Africa
  https://www.nature.com/articles/palcomms201669 (Academic paper)
- How do we effectively cover image-based abuse as gender-based violence, African Feminism
  https://africanfeminism.com/how-do-we-effectively-cover-image-based-abuse-as-gender-based-violence-part-i


APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS


take back the tech