



CYBER VIOLENCE AGAINST WOMEN & GIRLS (CVAWG)

Non-Consensual Intimate Image Abuse



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

NCIIA DEFINITION

Have you ever heard the term "Revenge Porn"?



Ask the question and if participants say yes, ask them to tell you what it refers to.

NCIIA DEFINITION

Have you ever heard the term "Revenge Porn"?



What about the term Non-Consensual Intimate Image Abuse (NCIIA)?



Do not provide any input on their responses, but continue to ask them if they ever heard the term NCIIA.

NCIIA DEFINITION



Non-Consensual Intimate Image Abuse (NCIIA), often called “image-based sexual abuse” or wrongly referred to as “revenge porn,” is the creation, distribution, or threat to distribute intimate images or videos of someone without their consent.



Present the NCIIA definition and explain that the term revenge porn has been widely used, but it is wrong that's why it has been replaced.

NCIIA DEFINITION

Word Battles

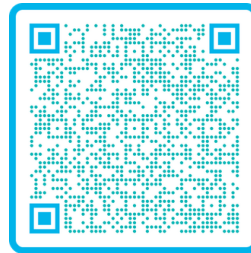
Group 1

Why do you think the term
"Revenge Porn" is wrong?



Group 2

Why is it more appropriate to
use the term "Non-Consensual
Intimate Image Abuse
(NCIIA)" ?



Divide participants into two groups:

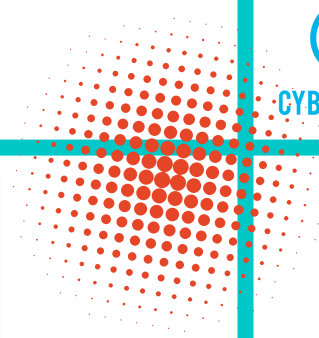
- * Group 1 = Revenge Porn
- * Group 2 = Non-Consensual Intimate Image Abuse

Give each group their question as shown in the slide and ask them to scan the QR code in order to record their answers.

*Alternatively print the handouts and give them to each group to complete.

NCIIA DEFINITION

Word Battles



ACTIVITY HANDOUT
2023-2-CY02-KA220-YOU-00018280

CyberEqual: Educating Youth on Cyber Violence Against Women & Girls

Revenge Porn vs. Non-Consensual Intimate Image Abuse

	Revenge Porn	Non-Consensual Intimate Image Abuse
Focus of the term		
Implied cause		
Who is blamed / responsible		
Perception of seriousness		
How victims might feel about this label		
Legal / social recognition		

Co-funded by the European Union

Give both groups the same criteria to analyze:

- * Focus of the term
- * Implied cause
- * Who is blamed / responsible
- * Perception of seriousness
- * How victims might feel about the label
- * Legal / social recognition

Instructions for groups:

“On your table, analyze your assigned term according to these six criteria. Think about what the words suggest, who they point to, and how they might affect perceptions. Be prepared to present back.”

Each group presents their analysis to the others (5 minutes per group).

Guide a conversation around these prompts:

- * What differences do you notice between the two terms?
- * Which term better reflects the harm done and why?
- * How might survivors experience these labels differently?
- * How can language influence whether society takes the issue seriously?

Responses to each column which can be used are accessible using the following link:
<https://docs.google.com/document/d/1FA4hnPIFf8NALx2WgrUuXgipsdJ5wT6N2y7wOsic66E/edit?usp=sharing>

NCIIA DEFINITION

Word Battles

Why "Revenge Porn" is Misleading & Harmful



Recap conclusion:

It trivialises the abuse

- * The word "porn" suggests entertainment or consensual sexual content, when in fact the core issue is non-consensual abuse and violation of privacy.
- * It risks normalising or sensationalising the harm.

It misrepresents motive

- * "Revenge" implies the perpetrator is justified or acting in retaliation, which shifts focus away from the criminal nature of the act.
- * Not all cases involve "revenge" – many involve coercion, extortion, humiliation, or profit motives.

It contributes to victim-blaming

- * The framing makes it seem like the victim did something to "deserve" revenge.
- * Survivors often internalise this language, feeling shame or responsibility.

It obscures gendered patterns of violence

- * Most victims are women and girls, while most perpetrators are men. Calling it "revenge" hides the power imbalance and gender-based violence dimension.

It undermines legal recognition

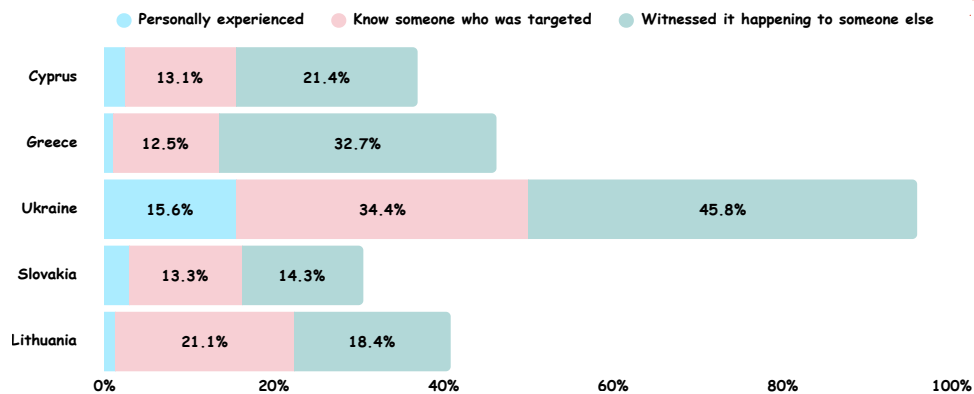
- * Using "porn" instead of "abuse" can make it harder for survivors to be taken seriously in courts, workplaces, or communities.
- * Legal and advocacy communities prefer terms like "Non-Consensual Intimate Image Abuse"

(NCIIA)” or “image-based sexual abuse”, which correctly frame it as abuse, not entertainment.

PREVALENCE OF NCIIA



CyberEqual Survey



According to recent studies, nearly 1 in 3 women worldwide have experienced some form of gender-based violence.

And with the rise of digital technology, many face violence online too, from harmful messages to threats.

The CVAWG survey was implemented in the context of the 'CyberEqual' project, a project co-funded by the Erasmus+ Programme of the European Union, aiming to map the prevalence of Cyber Violence Against Women and Girls in Cyprus, Greece, Ukraine, Slovakia and Lithuania. 467 women, aged 15 to 35 years old, participated in the study 76% of them reporting having experienced, witnessed, or knowing someone who experienced CVAWG.


In terms of NCIIA the prevalence per country is shown in the current figure.

These numbers show that CVAWG isn't just happening in one place; it's a global problem affecting millions across different countries and communities.

LEGAL FRAMEWORK



	Europe	Council of Europe's Istanbul Convention (Article 40 on sexual harassment, including online).
	Cyprus Greece Ukraine Slovakia Lithuania	EU Digital Services Act & Code of Conduct on Countering Illegal Hate Speech Online.



****Partners should include their country's legislation on the threat addressed (replace the question mark, the flag and keep their country's name on the box). Another slide maybe added if necessary.****

One key part of the Directive is protecting victims. It requires countries to provide support like legal help, counseling, and emergency aid for people affected by tech-related violence. It also makes sure victims' privacy is protected during legal cases and that easy ways to report online abuse are available.

Article 5(b) of the EU GBV Directive criminalises sharing non-consensual intimate or altered images but focuses mainly on explicit sexual content and wide sharing. This can be too limited.

It's important to recognise that non-explicit or culturally sensitive images (like partial nudity or private cultural moments) can also harm people. We need a broader and more sensitive definition of "intimate image" to better protect different communities and respect diverse views of privacy and harm.

GDPR provides strong protections for personal data, including intimate images. Sharing such images without consent is an unlawful processing of sensitive personal data. Victims can demand erasure ("right to be forgotten"), compensation, and sanctions against offenders.

DETANGLING NCIIA

Blurry Lines



Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

Is this NCIIA?

YES

NO



Tell participants: “I’ll read you a story in stages. After each part, you decide: Is this NCII? Answer YES or NO.”

Stage 1

Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

Is this NCII?

Correct answer: NO – this is consensual sharing.

After their breakup, Mark uploads Anna’s intimate photo online without asking her.

Is this NCII?

Correct answer: YES – this is non-consensual intimate image abuse.

Stage 3

Mark also forwards Anna’s intimate photos to a group chat with his friends, again without her permission.

Is this NCII?

Correct answer: YES – still NCII, because the images were shared without consent.

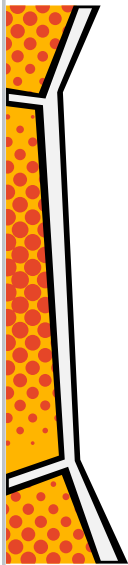
Later, someone takes Anna’s holiday pictures from Facebook. Using AI, they create a fake pornographic video of her and spread it online.

Is this NCII?

Correct answer: NO – this is not NCII in the traditional sense, because no real intimate photo was shared. BUT it is still abuse – this is called DEEPFAKE ABUSE.

DETANGLING NCIIA

Blurry Lines



Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

After their breakup, Mark uploads Anna's intimate photo online without asking her.

Is this NCIIA?

YES

NO



Tell participants: "I'll read you a story in stages. After each part, you decide: Is this NCII? Answer YES or NO."

Stage 1

Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

Is this NCII?

Correct answer: NO – this is consensual sharing.

After their breakup, Mark uploads Anna's intimate photo online without asking her.

Is this NCII?

Correct answer: YES – this is non-consensual intimate image abuse.

Stage 3

Mark also forwards Anna's intimate photos to a group chat with his friends, again without her permission.

Is this NCII?

Correct answer: YES – still NCII, because the images were shared without consent.

Later, someone takes Anna's holiday pictures from Facebook. Using AI, they create a fake pornographic video of her and spread it online.

Is this NCII?

Correct answer: NO – this is not NCII in the traditional sense, because no real intimate photo was shared. BUT it is still abuse – this is called DEEPFAKE ABUSE.

DETANGLING NCIIA

Blurry Lines



Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him. After their breakup, Mark uploads Anna's intimate photo online without asking her.

Mark also forwards Anna's intimate photos to a group chat with his friends, again without her permission.

Is this NCIIA?

YES

NO



Tell participants: "I'll read you a story in stages. After each part, you decide: Is this NCII? Answer YES or NO."

Stage 1

Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

Is this NCII?

Correct answer: NO – this is consensual sharing.

After their breakup, Mark uploads Anna's intimate photo online without asking her.

Is this NCII?

Correct answer: YES – this is non-consensual intimate image abuse.

Stage 3

Mark also forwards Anna's intimate photos to a group chat with his friends, again without her permission.

Is this NCII?

Correct answer: YES – still NCII, because the images were shared without consent.

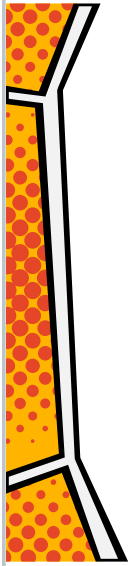
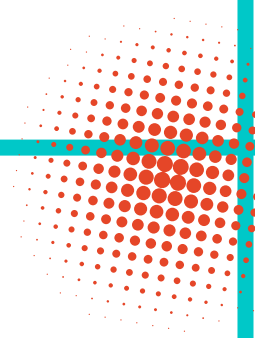
Later, someone takes Anna's holiday pictures from Facebook. Using AI, they create a fake pornographic video of her and spread it online.

Is this NCII?

Correct answer: NO – this is not NCII in the traditional sense, because no real intimate photo was shared. BUT it is still abuse – this is called DEEPFAKE ABUSE.

DETANGLING NCIIA

Blurry Lines



Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him. After their breakup, Mark uploads Anna's intimate photo online without asking her.

Mark also forwards Anna's intimate photos to a group chat with his friends, again without her permission.

Later, someone takes Anna's holiday pictures from Facebook. Using AI, they create a fake pornographic video of her and spread it online.

Is this NCIIA?

YES

NO



Tell participants: "I'll read you a story in stages. After each part, you decide: Is this NCII? Answer YES or NO."

Stage 1

Anna and Mark are dating. Anna sends Mark a private intimate photo because she trusts him.

Is this NCII?

Correct answer: NO – this is consensual sharing.

After their breakup, Mark uploads Anna's intimate photo online without asking her.

Is this NCII?

Correct answer: YES – this is non-consensual intimate image abuse.

Stage 3

Mark also forwards Anna's intimate photos to a group chat with his friends, again without her permission.

Is this NCII?

Correct answer: YES – still NCII, because the images were shared without consent.

Later, someone takes Anna's holiday pictures from Facebook. Using AI, they create a fake pornographic video of her and spread it online.

Is this NCII?

Correct answer: NO – this is not NCII in the traditional sense, because no real intimate photo was shared. BUT it is still abuse – this is called DEEPFAKE ABUSE.

DETANGLING NCIIA

Blurry Lines



How does the deepfake example show us that technology can create new forms of image-based abuse, even without real intimate photos?



Pose the question at the assembly and invite participants to discuss it openly without providing any affirmative answers yourself.

DETANGLING NCIIA

Blurry Lines

Deepfakes



An image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.



Even if the images/videos are fake, the harm is real!



The deepfake example shows that abuse doesn't require an actual intimate photo – perpetrators can now create fake sexualised images or videos using AI.

This highlights how technology evolves abuse tactics, expanding the risks survivors face.

Even if the images are fake, the harm is real: reputational damage, stigma, fear, and trauma.

It reinforces the need for laws (like the new EU Directive) to cover manipulated images, not just real ones.

Imagine your best friend tells you that their private intimate images were shared online without their consent.

What do you think happens next in their life; how might they feel, how might others treat them, and what challenges could they face?



Split participants into 3 groups (the psychological harm group, social impact group and the professional impact group) and ask them to respond to the question using the MentiMeter link.

Discuss their responses.

NCIIA IMPACT



Psychological harm

Shame
Anxiety
Depression
PTSD
Suicidal Ideation

Social impact

Stigma
Victim-blaming
Isolation
Damaged Relationships

Professional impact

Career setbacks
Withdrawal from Education/Work
Reputational Damage



Long-term harm: Content may remain online indefinitely, resurfacing repeatedly.

Finally, show them the impacts of NCIIA noting the ones they already identified.

COPING WITH NCIIA



Emotional Coping

Acknowledge your feelings: It's normal to feel anger, fear, shame, or sadness. Allowing yourself to feel them is part of healing.

Challenge self-blame: The responsibility lies entirely with the person who shared or threatened to share your images without consent.

Seek support: Talk with trusted friends, family, or a therapist. Having someone who validates your experience helps reduce isolation.

Document everything: Take screenshots of posts, threats, usernames, dates/times. Don't engage with the abuser more than necessary – but preserve evidence.

Report & takedown:

* Many social media platforms (Facebook, Instagram, TikTok, Twitter, etc.) have dedicated tools to report intimate image abuse.

* In the EU and some other regions, there are hotlines to help remove content quickly (e.g., StopNCII.org).

* Report to the police, especially if there are ongoing threats.

Safeguard online accounts: Change passwords, enable 2FA, and consider tightening privacy settings.

REPORTING OF NCIIA



Report to police

Report to the cybercrime unit, or national hotline.

Greece

Hellenic Cybersecurity Unit



11188 / 21 4402 7860



<https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/kataggelies/kataggelia-gia-parabiase-tou-aporretou-ton-elektronikon-kai-telephonikon-epikoinonion>



ccu@cybercrimeunit.gov.gr

Report to online platforms

Report to platforms such as Instagram, X, Tik Tok, Facebook etc.

On each platform, follow the instructions available for reporting the incident(s) and request the content to be removed.

*** Remember to keep screenshots before requesting removal.**



**** Each partner should replace the country, police unit and contact details.****

Reporting non-consensual intimate image abuse is a crucial step in regaining control and seeking justice. There are several avenues available to report these incidents effectively.

First, you can report directly to the police or your national cybercrime hotline.

Additionally, online platforms play a vital role. Platforms like Instagram, X, TikTok, and Facebook have built-in reporting mechanisms. Always follow their instructions to report the incident and request content removal.

***Remember, before initiating a takedown request, take screenshots to preserve evidence.**

This evidence is crucial for any ongoing investigations and can help prevent further harm. Taking these steps not only aids in your own protection but also contributes to a safer digital environment for others.

Remember, taking action is empowering, and you are not alone in this process.

PREVENTION OF NCIIA



Think critically before sharing

Consider who you're sharing with, how well you trust them, and whether the platform offers privacy protections.

Understand digital permanence

Even if an app offers disappearing messages, screenshots and screen recording can bypass these protections.

Password hygiene

Use strong, unique passwords and enable multi-factor authentication (MFA) for devices, cloud storage, and social media.

Device security

Keep phones and laptops locked with PINs or biometric authentication.

Private storage

If intimate images are kept, store them in encrypted folders or secure drives rather than default galleries.

Know reporting channels

Familiarize yourself with how to report NCIIA to platforms in case of misuse.

Evidence preservation

Learn how to safely capture and store digital evidence (screenshots, metadata) if needed later.

Stay updated

Keep informed about emerging threats like deepfake abuse and AI-generated images, which are increasingly common.



Present prevention measures

In groups, ask participants to design a TikTok script to be used for raising awareness on NCIIA.

*Alternatively, hand out pieces of paper or prepare a MentiMeter so that they can add their text for the TikTok script. If possible, ask them if they'd like to run it on TikTok.

**If a TikTok script is not applicable, they can design an NCIIA prevention poster.



RED CARD TO HARASSMENT

Accept - Report



Materials Needed:

Red and yellow cards (paper or actual cards) for each participant. The facilitators should print a yellow and red card x the number of groups they want to make.

How to Play:

The facilitators will read out different scenarios or behaviors, one by one.

Participants decide: If they believe the scenario is harassment, they raise their red card to report. If they want simply to reject it, they raise the yellow card. If they accept it, they don't raise any card.

After each one, ask the group:

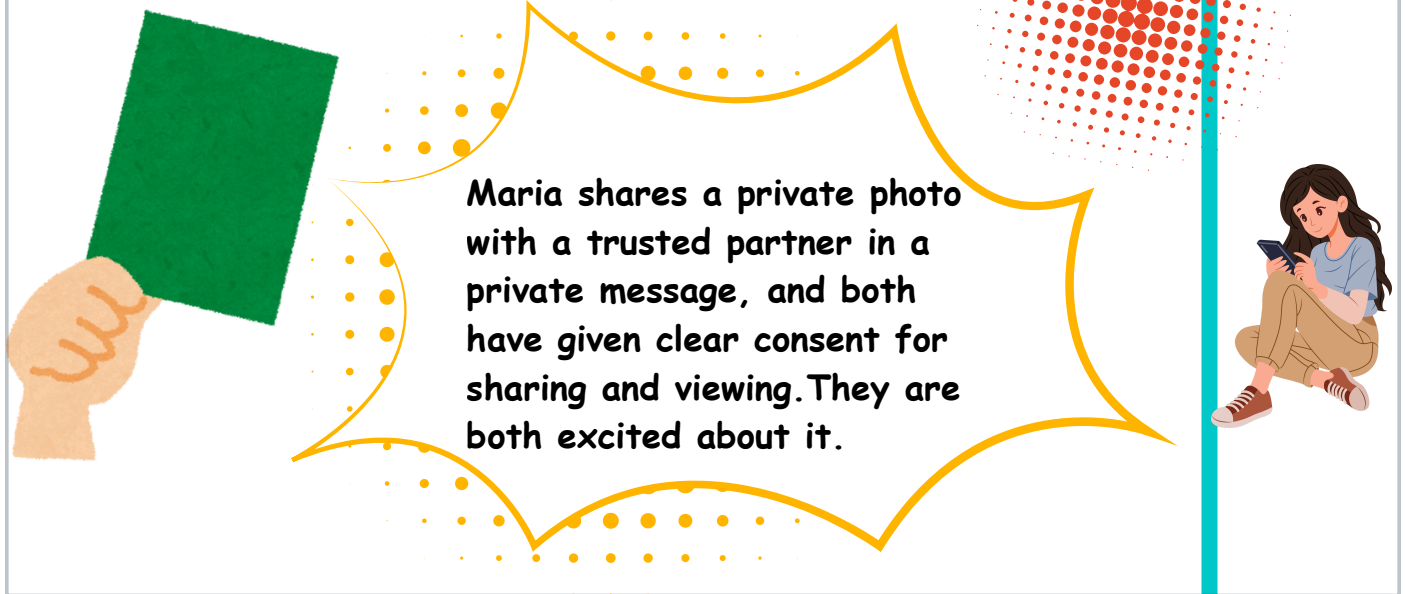
Why did you raise (or not raise) your red/yellow card?

How might this behavior affect someone?

Is this kind of behavior acceptable online or offline? Why?

Maria shares a private photo with a trusted partner in a private message, and both have given clear consent for sharing and viewing. They are both excited about it.



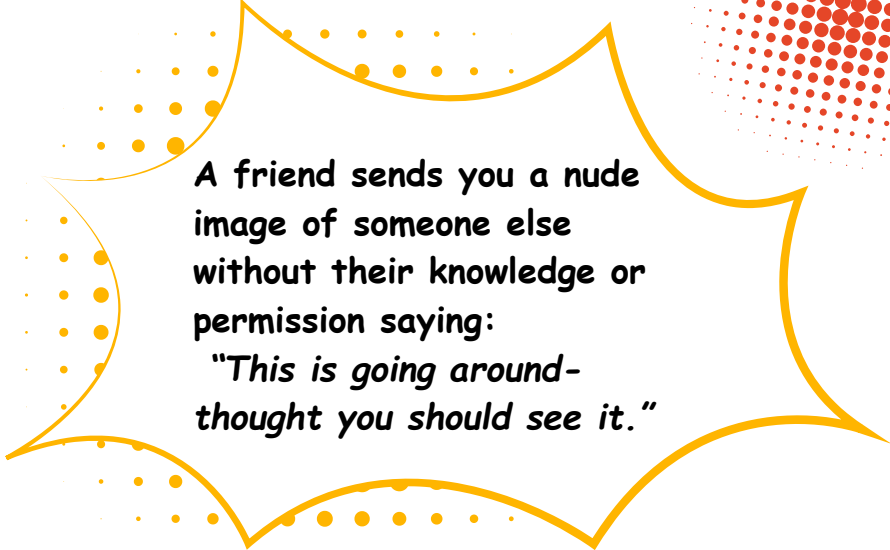


Private message in a trusted -security friendly- platform.

This is not harassment. It involves clear, mutual consent.

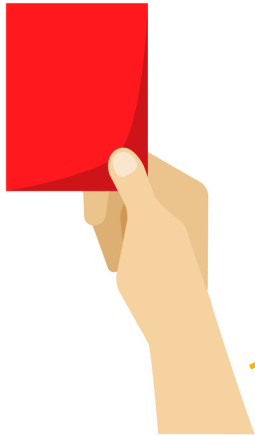
Consent was given by both people, and no one is being pressured or harmed. Sharing private content is only okay when everyone involved agrees willingly.

Accept.

A large, yellow, multi-pointed speech bubble with a dotted pattern along its edges, containing text.

A friend sends you a nude image of someone else without their knowledge or permission saying:
*"This is going around-
thought you should see it."*





A friend sends you a nude image of someone else without their knowledge or permission saying:
*"This is going around-
thought you should see it."*



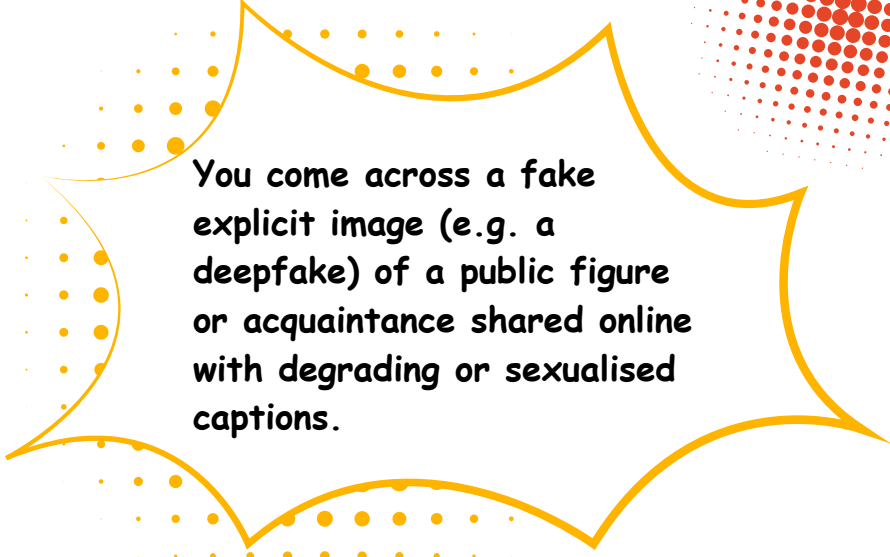
Yes, this is harassment and a form of Non-Consensual Intimate Image Abuse (NCIIA). The person in the image did not give consent to share it.

Forwarding such content is harmful, violates privacy, and may be illegal.

Even if someone else started it, sharing it again continues the harm.

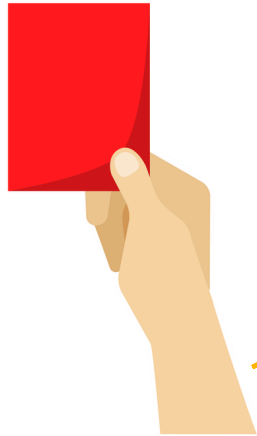
Always stop and report this kind of behavior- don't participate in it.

Report.

A large, yellow, multi-lobed speech bubble with a dotted pattern of small yellow dots inside, containing the text.

You come across a fake explicit image (e.g. a deepfake) of a public figure or acquaintance shared online with degrading or sexualised captions.





You come across a fake explicit image (e.g. a deepfake) of a public figure or acquaintance shared online with degrading or sexualised captions.



This is harassment and a form of image-based abuse. Even though the image is fake, it is meant to shame, humiliate, or sexually objectify someone.

Deepfakes can cause real emotional harm and damage someone's reputation or safety. This behavior is non-consensual, often targeting women and marginalised groups.

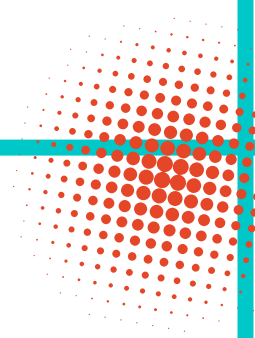
Sharing or supporting this content fuels CVAWG.

Report.



CYBEREQUAL

THANK YOU!



CVAWG IS REAL VIOLENCE!



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.