ENDTAB.ORG

DEEPFAKES
a victim resource guide

GUIDE OVERVIEW

This guide includes resources, tools and strategies for anyone who has been targeted by a **deepfake**, or similar technology, which has made it falsely appear they were in a pornographic video that they were not actually in.
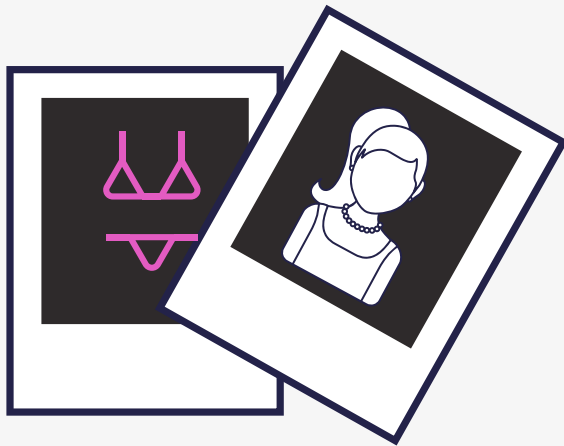

ORIGINAL   DEEPFAKE

CREDIT: FACEBOOK

YOU ARE NOT ALONE

96% of all deepfake videos are pornographic and almost all of these target women. However, this is a pervasive new form of online sexual abuse that threatens anyone, regardless of gender. And because this technology is new, some people may not be aware of deepfakes yet and there may not be laws against deepfake pornography in your state.

This means you may need to educate others when seeking help. This guide, and the accompanying fact sheet, is designed to help you with that.

1 SAVING THE EVIDENCE

Before deleting anything, be sure to preserve any evidence. Some ways to do this: (1) Download the video(s); (2) Screenshot the webpage, including the url, date & time and (3) Save the webpage as a pdf. Visit withoutmyconsent.org to utilize their evidence preservation **resources** for nonconsensual pornography (also effective for deepfake pornography).

2 REMOVE FROM GOOGLE SEARCHES

Google enables victims of nonconsensual deepfake pornography (referred to as 'involuntary fake pornography' by Google) to remove the offending video from appearing in their search results. [It does not mean it is removed from the actual website.] Click **here** to begin.

INSTAGRAM
YAHOO
FACEBOOK
GOOGLE
TWITTER
SNAPCHAT
REDDIT
TUMBLR
PORNHUB

3 TAKE DOWN REQUESTS

Upon request, many technology platforms will remove a post (like nonconsensual pornography) because it violates their content policies. Nonconsensual deepfake pornography should be treated similarly. The Cyber Civil Rights Initiative created content removal guides for any of the sites listed on the left (click any of them to start the process) or to see the entire guide, visit: www.cybercivilrights.org/online-removal/

4 TAKE DOWN REQUESTS:
COPYRIGHT

A deepfake of Kim Kardashian was removed from YouTube based on a copyright take down request from the company that created the original video. It may be possible to apply this approach to deepfake pornography by contacting the publisher of the underlying pornographic video. They may be able to issue a copyright take down notice. Or you may seek to issue the take down notice yourself following the same approach used for nonconsensual pornography **here**. We recommend speaking with an attorney if you have questions.

CALIFORNIA
+
VIRGINIA

5 DEEPFAKE LAWS:
PORNOGRAPHY

States are slowly beginning to pass laws that specifically address nonconsensual deepfake pornography. Virginia updated its criminal nonconsensual pornography law to include deepfakes. California passed a law that allows a victim to sue civilly. Click either state to the left to view the relevant law.

6 EXISTING CRIMINAL LAWS

When reporting deepfake pornography to law enforcement, they may need to rely on existing criminal laws until specific deepfake laws are passed. Some suggested laws are listed to the right.
NOTE: Nonconsensual pornography (Revenge Porn) laws will likely not apply because they require the victim's body (not just their face) appear in the video.

FALSE IMPERSONATION
HARASSMENT
EXTORTION
IDENTITY THEFT
CREDIBLE IMPERSONATION
DOMESTIC VIOLENCE

7 RESTRAINING ORDERS

You may choose to seek a restraining order requesting that the restrained party take down, destroy and not distribute the deepfake (or create any new deepfakes). For purposes of seeking a restraining order, nonconsensual deepfake pornography may be categorized as harassment, disturbing your peace, false impersonation, threatening behavior, inflicting emotional distress and more. Contact your local domestic violence or sexual assault organization for assistance.

SAMPLE LANGUAGE:

I am the victim of a new form of online abuse called nonconsensual 'deepfake' pornography. These deepfake videos use face-swapping software or an app to transfer a victim's face onto the body of someone else in a pornographic video, making it appear the victim was in a video they were not in fact in. [Name of Restrained Party], using only images of my face, created and/or distributed/is threatening to distribute a pornographic deepfake video of me without my consent. It looks like me in the video, but it is not me. [Name of Restrained party] possesses many images of me, meaning there is nothing to stop him/her/them from continuing to manufacture more fake pornographic videos of me at will.

EXPLAINING DEEPFAKES

EXPLAINING THE HARM

WHEN VIEWERS BELIEVE IT'S REAL

When the deepfake is believed to be authentic, the harm caused is similar to that of nonconsensual pornography. Distribution can adversely impact a person's employment, reputation, relationships, emotional well-being and upend their life. Never knowing when or if a deepfake will show up can leave victims in a perpetual state of anxiety and fear.

WHEN VIEWERS KNOW IT'S FAKE

Nonconsensual deepfake pornography does not have to be believed to cause harm. Even if labeled as fake, a pornographic deepfake that is shared and watched by others is an act that sexualizes and fetishizes a victim publicly without their consent. This form of exploitation can destroy the fundamental building blocks a person needs in order to thrive.

DEEPFAKE FACT SHEET

WHAT IS NONCONSENSUAL DEEPFAKE PORNOGRAPHY?
These videos use face-swapping technology to transfer a victim's face onto the body of someone else in a pornographic video, making it falsely appear the victim is engaging in sex acts. These videos are created and/or shared without the victim's consent.   To safely see how this technology works, click **here** to watch an explanatory video created by Facebook.

CREDIT: FACEBOOK

WHO CAN CREATE A DEEPFAKE? Anyone. This technology uses artificial intelligence to empower any layperson with the ability to make realistic fake videos. Alternatively, someone can also commission the creation of a deepfake on any number of different websites.

WHAT IS THE HARM? The harm is two-fold. The first layer of harm occurs when a deepfake pornographic video is believed to be authentic. Much like nonconsensual pornography, in this circumstance a victim's reputation, relationships, emotional health and more are impacted. The second layer of harm occurs when viewers know the video is fake, but watch it anyway. In this circumstance, victims are still being fetishized and sexualized without their consent which can compromise their emotional health, make them feel unsafe and more. To be clear, debunking or detecting a deepfake does NOT mitigate this second layer of harm for the victim.

WHAT IS THE IMPACT?   Per the most recent **report** by Deeptrace Labs, deepfake pornography is exploding in popularity. In 2019, the total number of deepfakes more than doubled over a 9 month period to nearly 15,000, and 96% of them are pornographic. To date, across just four websites, deepfake pornography videos have garnered 134,364,438 unique views and counting. The report also found that nearly 100% of all deepfake pornography targets women.

IS THERE A TECH SOLUTION? No. As of now, there is no reliable way to detect deepfakes with 100% certainty. And, as mentioned above, detection does not eliminate the second layer of harm to victims of nonconsensual deepfake pornography.

WHAT HAS BEEN THE LEGAL RESPONSE? In June 2019, The House Intelligence Committee held a **hearing** to examine the public risks posed by deepfake videos. Also in 2019, three states - California, Virginia and Texas - passed 4 deepfake laws related to elections (California & Texas) and pornography (California & Virginia).

RESOURCES & LINKS

- DEEPFAKE RESOURCES -

EndTAB: End Technology-Enabled Abuse (endtab.org)
Live and online trainings and resources to address and prevent technology-enabled abuse - like nonconsensual deepfake pornography - perpetrated against victims of domestic violence, sexual assault, stalking, human trafficking and elder abuse.

Deepfake Domestic Violence Advisory (click here)
Co-authored by Erica Johnstone (withoutmyconsent.org) and Adam Dodge (EndTAB, @adamrdodge), this advisory provides guidance to address deepfake abuse within the context of domestic violence.

Deeptrace Labs (deeptracelabs.com)
Providing research and threat solutions to deepfakes, including publishing the State of Deepfakes Report.

Witness (witness.org)
Their project focuses on the emerging and potential malicious uses of so-called "deepfakes" and other forms of AI-generated "synthetic media" and how we push back to defend evidence, the truth and freedom of expression.

TED Talk by Danielle Citron (click here)
How Deepfakes Undermine Truth and Threaten Democracy.

Amber (ambervideo.co)
Providing solutions to authenticate and detect deepfakes and fake videos.

- NONCONSENSUAL PORNOGRAPHY RESOURCES -

Cyber Civil Rights Initiative (cybercivilrights.org)

Without My Consent (withoutmyconsent.org)

BADASS Army (badassarmy.org)

K&L Gates's Cyber Civil Rights Legal Project: (cyberrightsproject.com)

- GENDER BASED VIOLENCE RESOURCES -

National Domestic Violence Hotline (thehotline.org)

National Network to End Domestic Violence (nnedv.org)

RAINN (Rape, Abuse & Incest National Network) (rainn.org)

Joyful Heart Foundation (joyfulheartfoundation.org)