Principles: Safety and security, Fairness and non-discrimination, Privacy, Human oversight and determination
Values: Human Rights
Stakeholders: Civil society, Public sector, Technical community

Falling Victim to AI enhanced Revenge Pornography

A woman discovers her ex-partner decided to exact revenge against her by uploading a video of her engaging in sexually explicit acts to a porn website.

The woman did not actually participate in the video; she realizes that it has been doctored and is distraught at how this video could impact her professional and personal life.

The link to the doctored video on the porn website has been sent to her co-workers, family and friends by her ex-partner.

The woman files a police report against her ex-partner in the meantime and inquires what legal action can be taken. She has not been physically assaulted but harmed through digital means. The police inform her she can take legal action against her ex-partner for revenge porn, and that she can also mediate with the porn website to take the video down. The website takes the original video content down, but pirated versions have already been made.

There are many legal challenges that arise in this case study relating to (1) copyright, given the fact that the original video has been modified, of (2) consent. Prosecution around deep fakes porn is complicated because deep fake porn is not real unless the user recognizes the face. Once the viewer recognizes the face, there is assumption that the incident occurred. Deep fake porn videos are a new form of sexual privacy invasion, which violates human dignity and autonomy.

- While legal action around deep fake porn is not yet concrete, we can encourage the porn sites in the private sector, in this case, porn sites to be proactive participants in regulating harmful content on their sites. For example, Porn hub recently reviewed its content uploading procedure and no longer accepts uploads from unverified users, will now publish regular transparency reports, and will also expand its content moderation efforts with the newly established ‘Red Team’ which will be solely responsible for vetting content on the platform.

- Legal authorities should move to resolve crimes of this nature through proper legal recourse such as copyright infringement, defamation, violation of privacy, appropriation of personality, or even harassment. However, legal recourse will vary on the jurisdiction of which the crime takes place.

- Members of civil society can reduce the risk of exposure to deep fakes by posting videos and selfies to private accounts or limiting the quantity and quality of public images and/or videos being shared online.

Privacy, safety & security, fairness and non-discrimination, human oversight & determination.

Know more about this case:

- “Regulating Deep Fakes: Legal and Ethical Considerations”, Vilnius University, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3497144

- “What Can The Law Do About ‘Deepfake'?”, Macmillian,https://www.mcmillan.ca/What-Can-The-Law-Do-About-Deepfake

- “The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective”, Sexuality & Culture, https://link.springer.com/article/10.1007/s12119-020-09738-0

- “The legal implications and challenges of deepfakes”, LexisNexis, https://www.dacbeachcroft.com/en/gb/articles/2020/september/the-legal-implications-and-challenges-of-deepfakes/

- “Pornhub bans unverified uploads, ability to download content from site”, The Hill, https://thehill.com/policy/technology/529325-pornhub-bans-unverified-uploads-ability-to-download-content-from-site