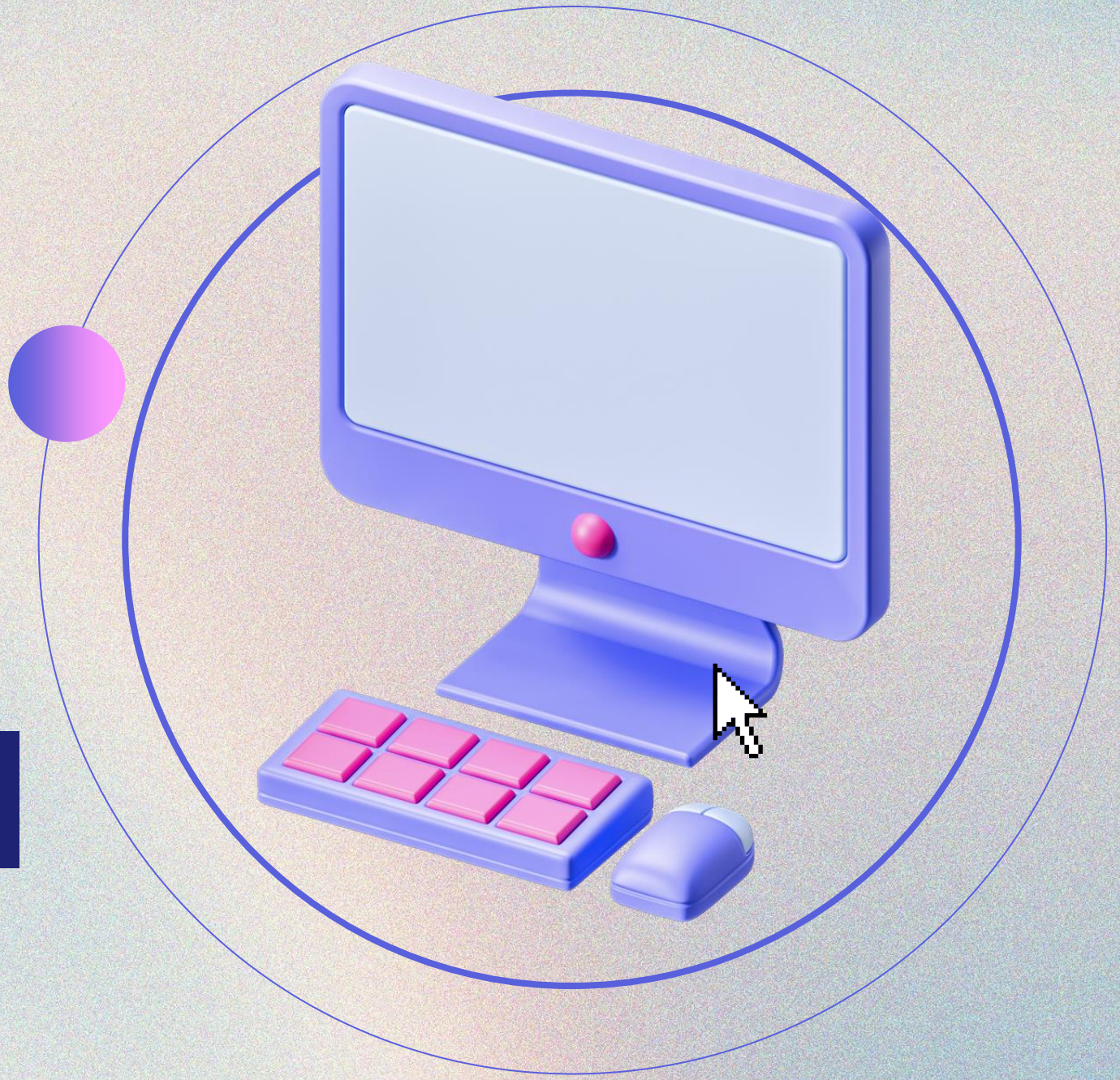
DEEPFAKES SYNTHETIC MEDIA GENERATIVE AI

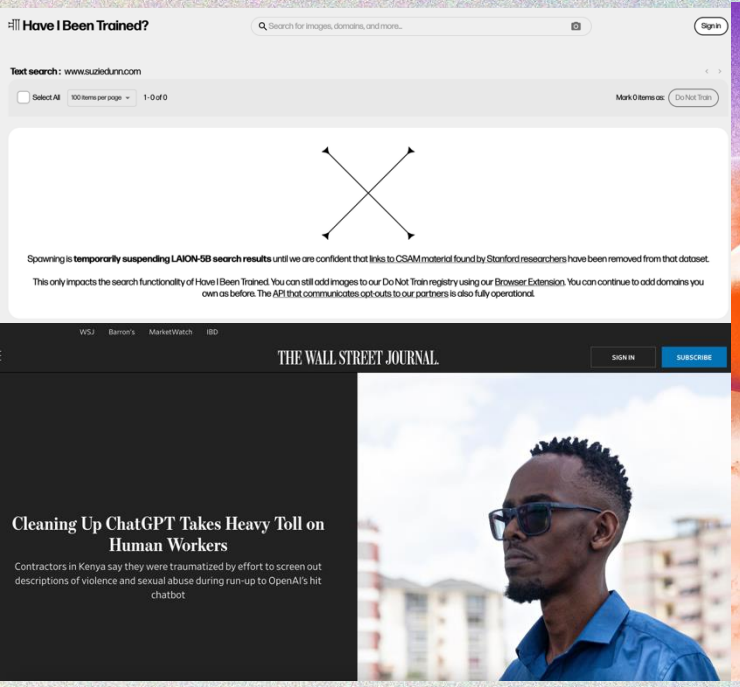


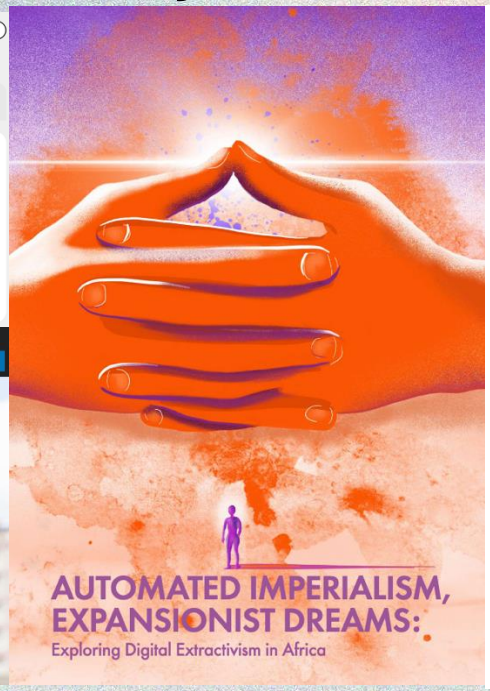
AI DEFINITIONS

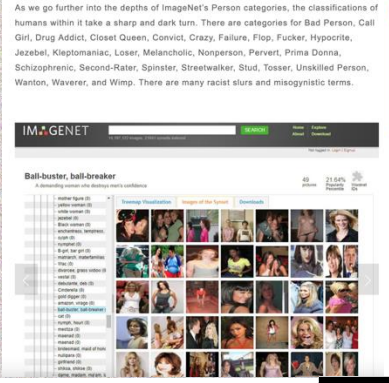
Artificial intelligence (“AI”) is defined “as a system that, using a model, makes inferences in order to generate output, including predictions, recommendations, or decisions
Generative Artificial Intelligence (“Gen-AI”) is “a type of artificial intelligence that is capable of generating new content, such as images or text, in response to a submitted prompt by learning from a large reference database of examples”
Large Language Models (“LLMs”) are a “form of Gen-AI that involves a computer program that uses very large collections of language data in order to understand and produce text” that matches patterns and responses to answers in a way to the way humans do.”
Synthetic media (“deepfakes”) visual, audio, and text-based content that has been created using a form of digital technology

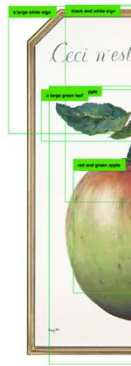
AI Basics: Training

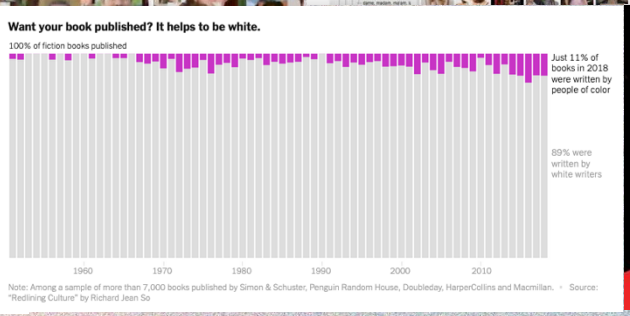
AI systems are trained on data that is labeled, can embed discrimination
Data scraping can potentially be violations of privacy and intellectual property

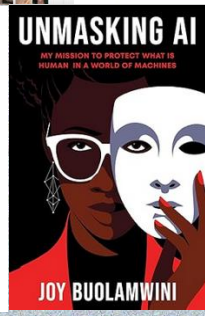




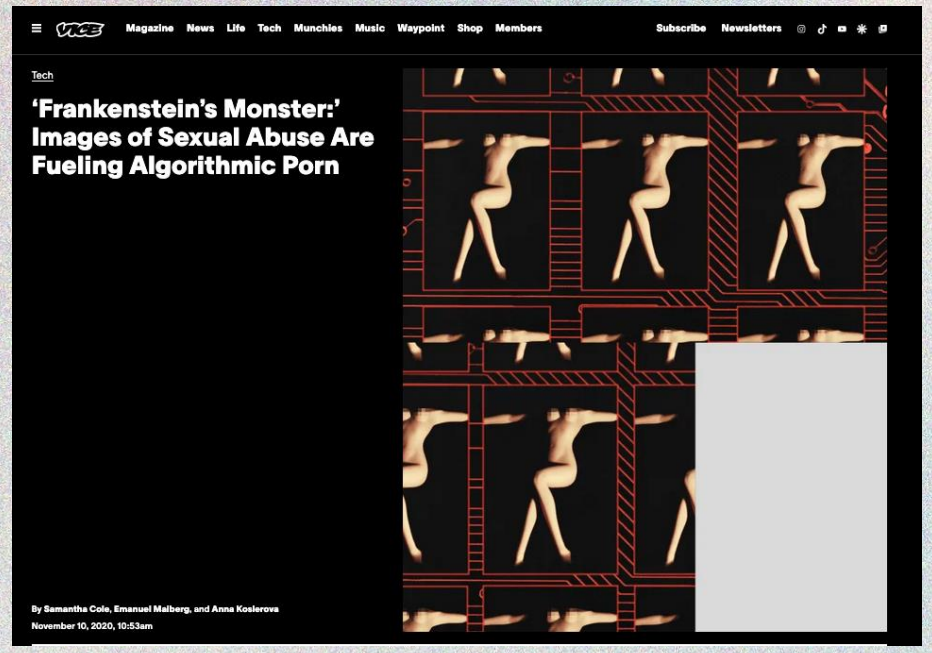






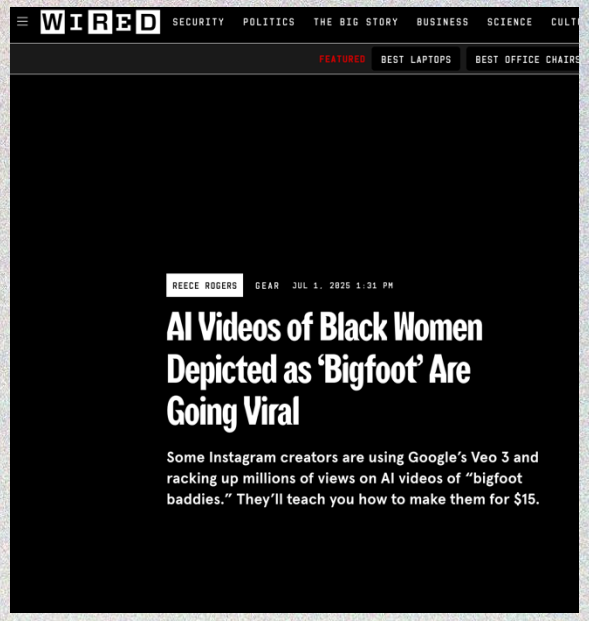


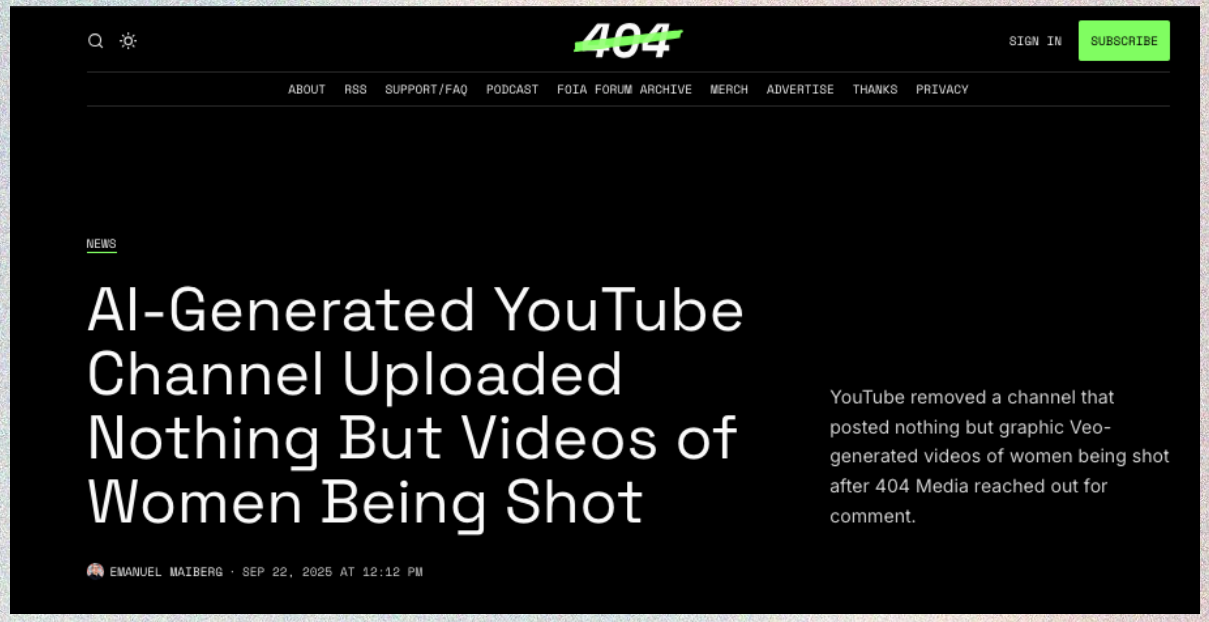
AI Basics: Training



AI Basics: Creating

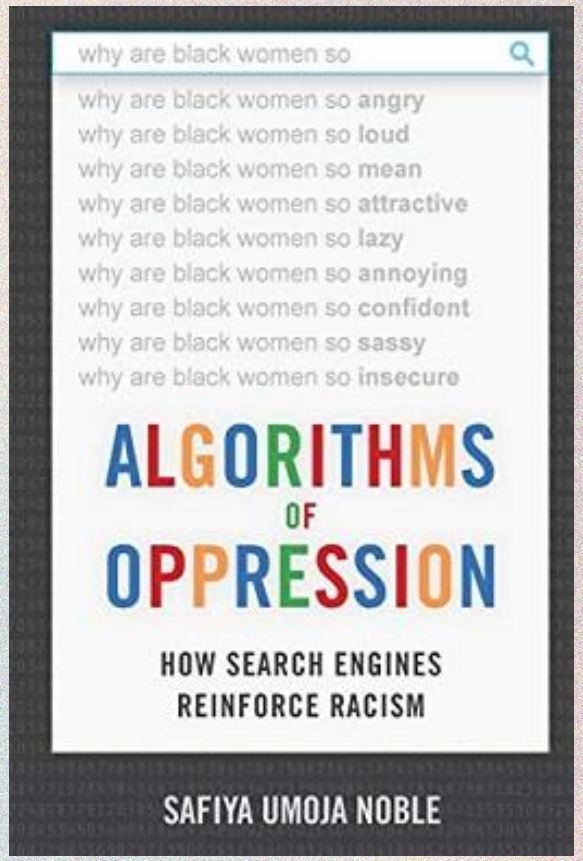
AI systems can be used to create harmful content
This can be done purposely by users or due to problems with the technology design

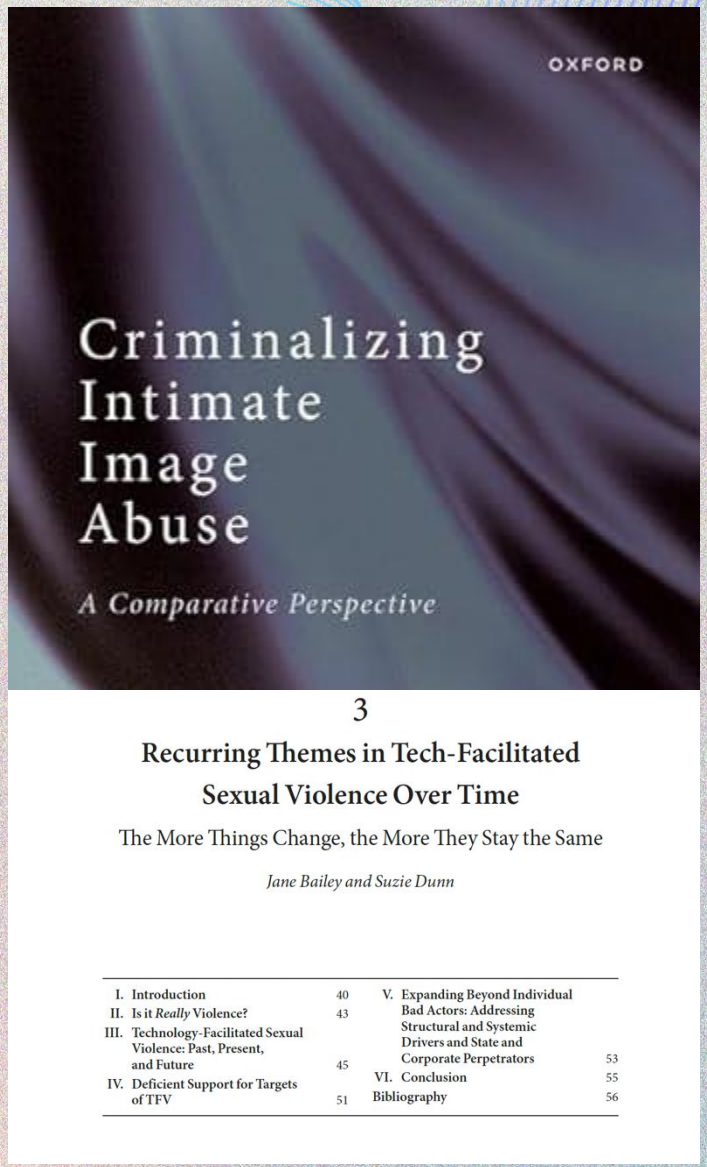




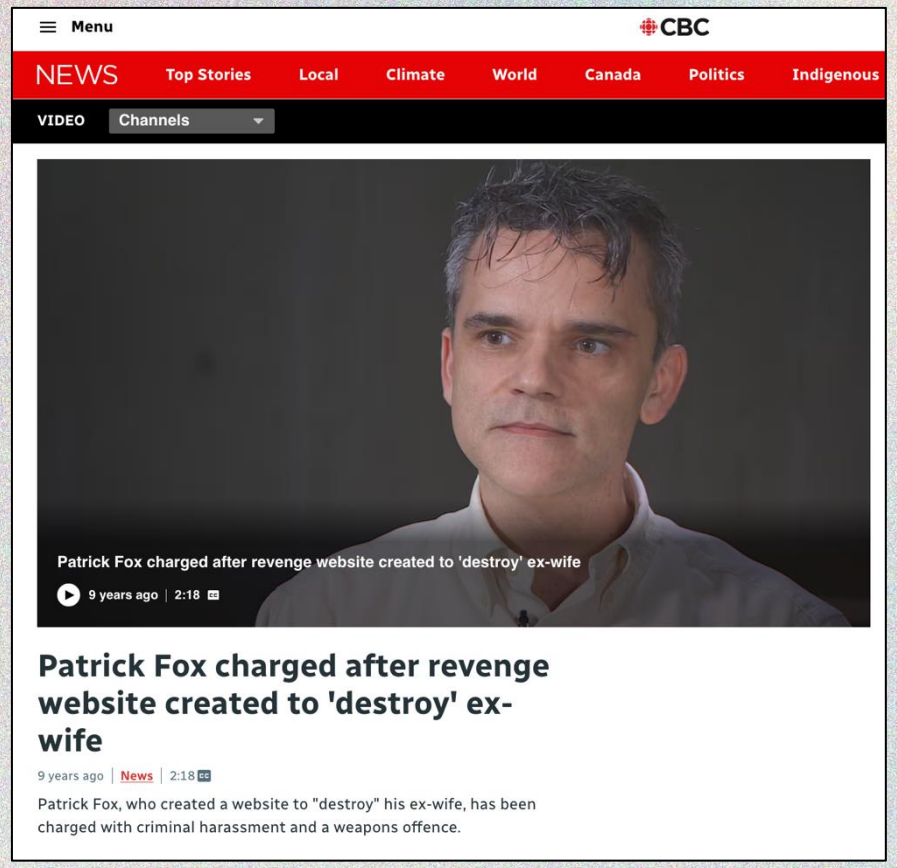
NOTHING NEW TO SEE HERE

- New technologies = old harms in new ways
- Searching “Black girls” turned up highly sexualized images
- Searches for professional hair of clothing for women, turned up white women
- Autofill resulted in sexist and racist results





FAKE CONTENT: LOW TECH

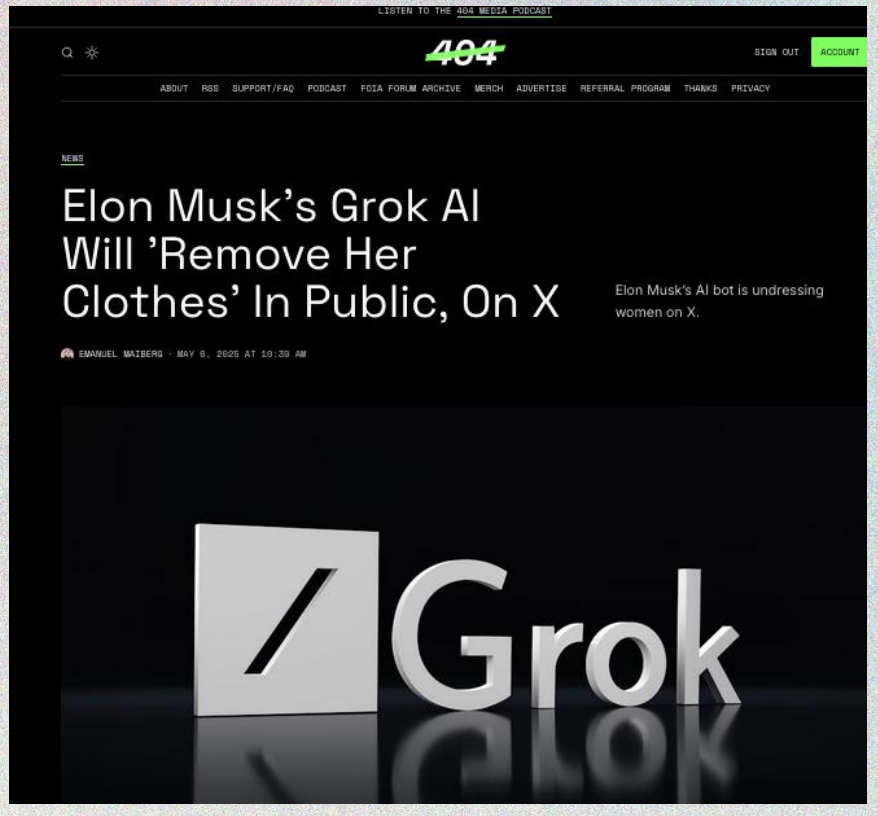


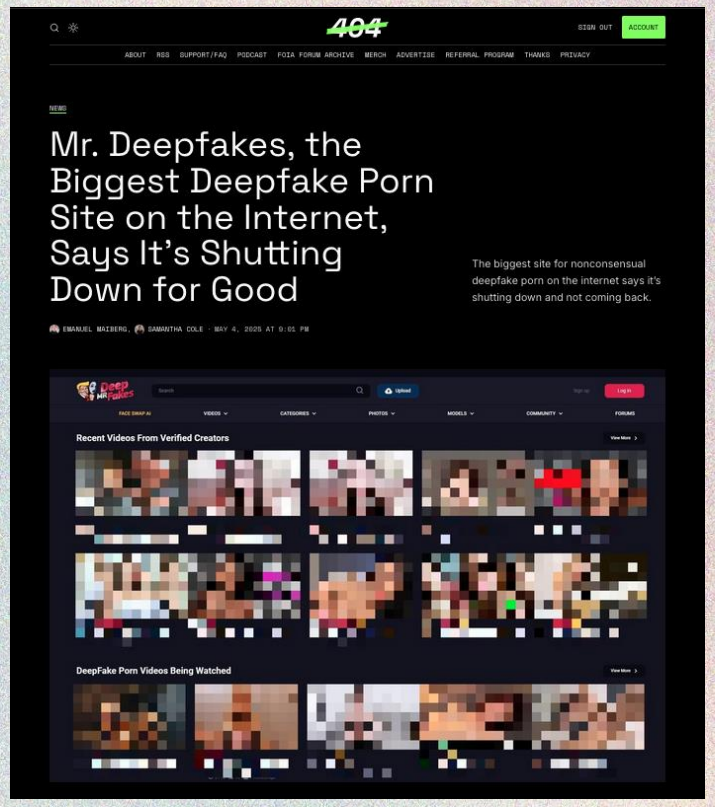
- *Lenihan v Shanker*, 2021 ONSC 330, appl'd 2021 ONCA 2021
  - High conflict family litigation
  - Forged emails allegedly from former spouse
  - Forged affidavits from witnesses
- *R v Fox*, 2017 BCSC 2361, appl'd 2019 BCCA 211
  - Family breakdown, years of ongoing false content
- *Yenovkian v Gulian*, 2019 ONSC 7279
  - Family breakdown, father made false claims about former spouse and children
- Photoshop to create CSAM
  - *R v Rhode*, 2019 SKCA 17; *R v CH*, 2010 ONCJ 270; *R v RMV*, 2015 BCPC 469; *R v GJM*, 2015 MBCA 103; *R v RK*, 2015 ONSC 2391

CURRENT AND FUTURE ISSUES

- Non-consensual synthetic intimate images (created and distributed)
- Impersonation or identity hacking via voice cloning and face swapping
- Gender-bias and sexism in AI chatbots, generative AI tools
- Spreading AI generated misinformation, algorithms promoting discriminatory content
- Altering existing content (changing context of emails, texts, editing photos)
- Creating fake content allegedly from/of a person (websites, text messages, events, images, email)
- Creating fake content allegedly from/of themselves (text messages, email, calendar dates, images, events)
- Content can be created to frame in both the negative and the positive
- Claims that content is faked (deepfakes, synthetic videos, voice cloning)

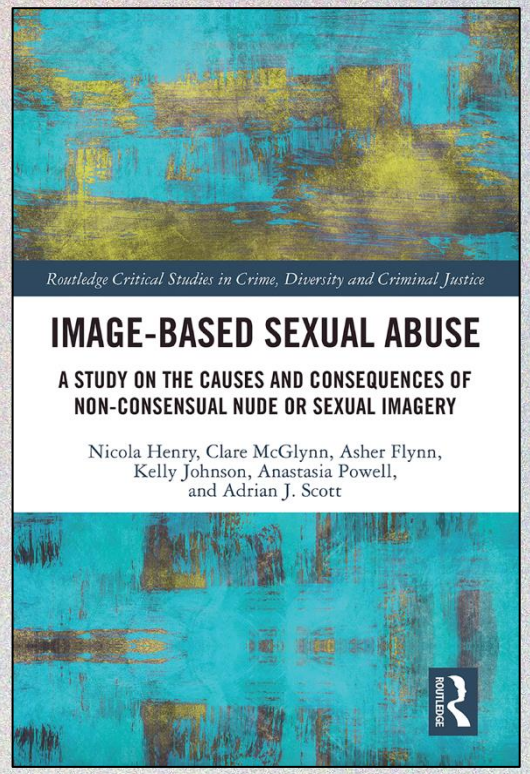
SEXUAL DEEPFAKES





- Deepfake (replace face in existing sexual video)
- Deepnude (replace with nude body in existing video)
- GenAI (create wholly new images or videos)
- Sextortion
- Child Sexual Abuse and Exploitation Material
- Harassment (public figures)
- Distribution without consent
- Creation without consent
- Hosting without consent
- Purpose built platforms
- Community learning spaces

SYNTHETIC SEXUAL CONTENT



Attitudes Towards and Knowledge of Non-Consensual Synthetic Intimate Imagery in 10 Countries

Rebecca Umbach
Google
USA

Nicola Henry
RMIT University
Australia

Gemma Beard
RMIT University
Australia

Colleen Berryessa
Rutgers University
USA

ABSTRACT

Deepfake technology tools have become ubiquitous, "democratizing" the ability to manipulate images and videos. One popular use of such technology is the creation of sexually explicit content, which can then be posted and shared widely on the internet. This article examines attitudes and behaviors related to non-consensual synthetic intimate imagery (NSII) across over 16,000 respondents in 10 countries. Despite nascent societal awareness of NSII, NSII behaviors were considered harmful. In regards to prevalence, 2.2% of all respondents indicated personal victimization, and 1.8% all of respondents indicated perpetration behaviors. Respondents from countries with relevant legislation also reported perpetration and victimization experiences, suggesting legislative action alone is not a sufficient solution to deter perpetration. Technical considerations to reduce harms may include suggestions for how individuals can better monitor their presence online, as well as enforced platform policies which ban, or allow for removal of, NSII content.

imagery" (NSII). One exception is when describing the language we used in the survey (where we used the more recognized "deepfake pornography" term).

The consumer creation of deepfakes started in late 2017 on Reddit, after a user named "deepfakes" posted NSII depicting the faces of female celebrities superimposed onto pornographic videos on his page [43, 80]. Continued consumer interest in NSII is reflected in the proliferation of dedicated NSII sites, often depicting celebrity targets. Abuse potential has increased in recent years as the technology has advanced in sophistication and availability [12, 34, 52, 79]. NSII can be considered a form of image-based sexual abuse because intimate images are created and/or shared without the consent of the person or persons depicted in the images. The harms of image-based sexual abuse have been well-documented, including negative impacts on victim-survivors' mental health, career prospects, and willingness to engage with others both online and offline [16, 38]. The proliferation of NSII technologies means that anyone can now become a victim of image-based sexual abuse, and research sug-

Journal of Digital Life and Learning
DOI: 10.51357/jdll.v3i1.218
2023, Vol. 3, No. 1, 1-21

Deepfakes and Harm to Women

JENNIFER LAFFIER[1], AALYIA REHMAN[1]

[1] *Ontario Tech University*

Abstract

As deepfake technologies become more sophisticated and accessible to the broader online community, their use puts women participating in digital spaces at increased risk of experiencing violence online and abuse. In a 'post-truth' era, the ability to discern what is real and what is fake allows malevolent actors to manipulate public opinion or ruin the social reputation of individuals to wider audiences. While the scholarly research on the topic is sparse, this study explored the harm women have experienced in technology and deepfakes. Results of the study suggest that deepfakes are a relatively new method to deploy gender-based violence and erode women's autonomy in their on-and-offline world. This study highlights the unique harms for women that are felt on both an individual and systemic level and the necessity for further inquiry into online harm through deepfakes and victims' experiences.

Keywords: Deepfakes, Women, Synthetic media, Image-based abuse, Harm

McGill Law Journal — Revue de droit de McGill

LEGAL DEFINITIONS OF INTIMATE IMAGES IN THE AGE OF SEXUAL DEEPFAKES AND GENERATIVE AI

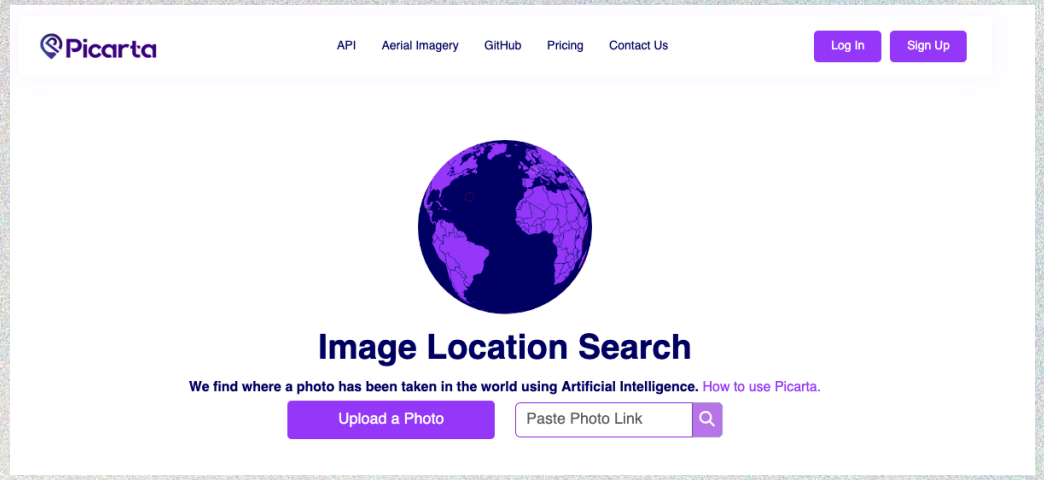
*Suzie Dunn**

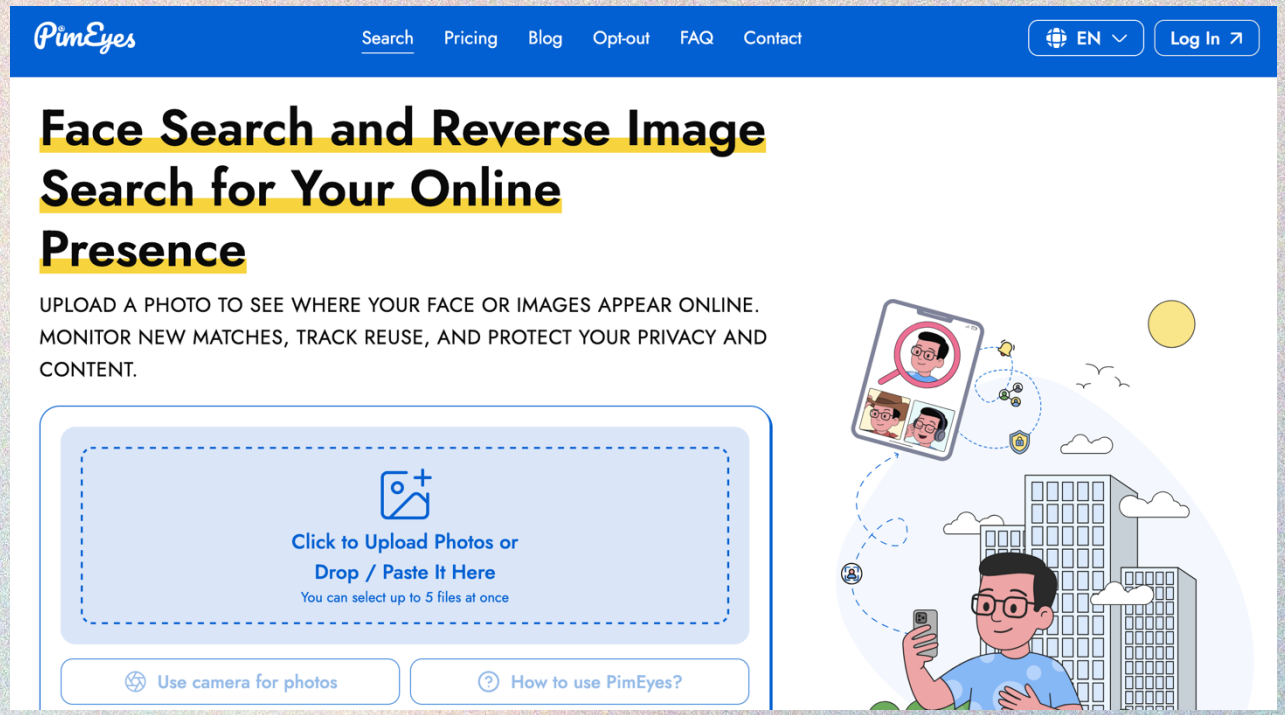
This article explores the evolution of Canadian criminal and civil responses to non-consensual synthetic intimate image creation and distribution. In recent years, the increasing accessibility of this type of technology, sometimes called deepfakes, has led to the proliferation of non-consensually created and distributed synthetic sexual images of both adults and minors. This is a form of image-based sexual abuse that law makers have sought to address through criminal child pornography laws and non-consensual distribution of intimate image provisions, as well as provincial civil intimate image legislation. Depending on the province a person resides in and the age of the person in the image, they may or may not have protection under existing laws. This article reviews the various language used to describe what is considered an intimate image, ranging from definitions seemingly limited to authentic intimate images to altered images and images that falsely present the person in a reasonably convincing manner.

Cet article explore l'évolution des réponses pénales et civiles canadiennes à la création et à la distribution d'images intimes synthétiques non consensuelles. Ces dernières années, l'accessibilité croissante de ce type de technologie, parfois appelée « deepfakes », a conduit à la prolifération d'images sexuelles synthétiques d'adultes et de mineurs créées et distribuées sans consentement. Il s'agit d'une forme d'abus sexuel par l'image que les législateurs ont cherché à combattre en adoptant des lois pénales sur la pornographie juvénile et des dispositions sur la distribution non consensuelle d'images intimes, ainsi que des lois civiles provinciales sur les images intimes. Selon la province dans laquelle une personne réside et l'âge de la personne figurant sur l'image, elle peut ou non bénéficier d'une protection en vertu des lois existantes. Cet article passe en revue les différents termes utilisés pour décrire ce qui est considéré comme une image intime, allant de définitions apparemment limitées à des images intimes authentiques à des images modifiées et à des images qui présentent faussement la personne d'une manière raisonnablement convaincante.

STALKING

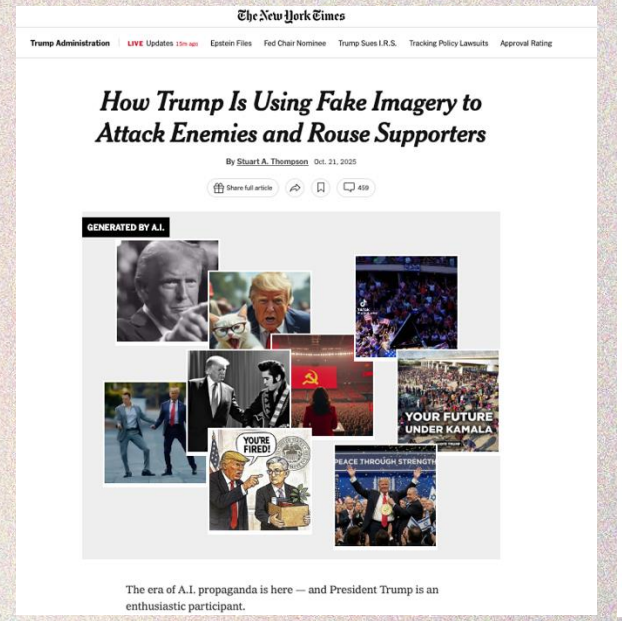
- Can use facial recognition technology to find a person online or identify them in real life
- Can use AI tools to determine where photos were taken

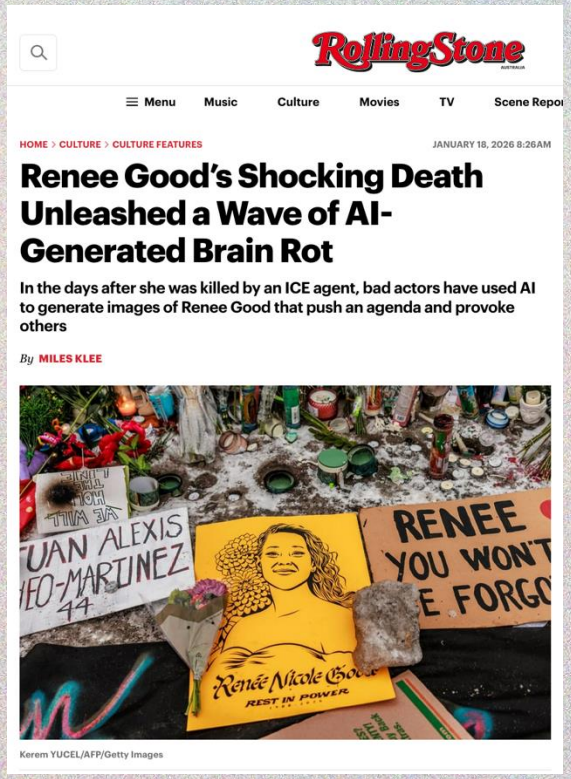


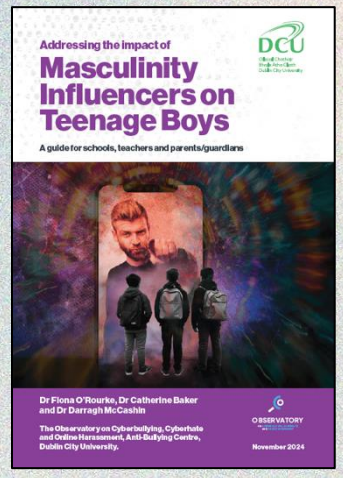


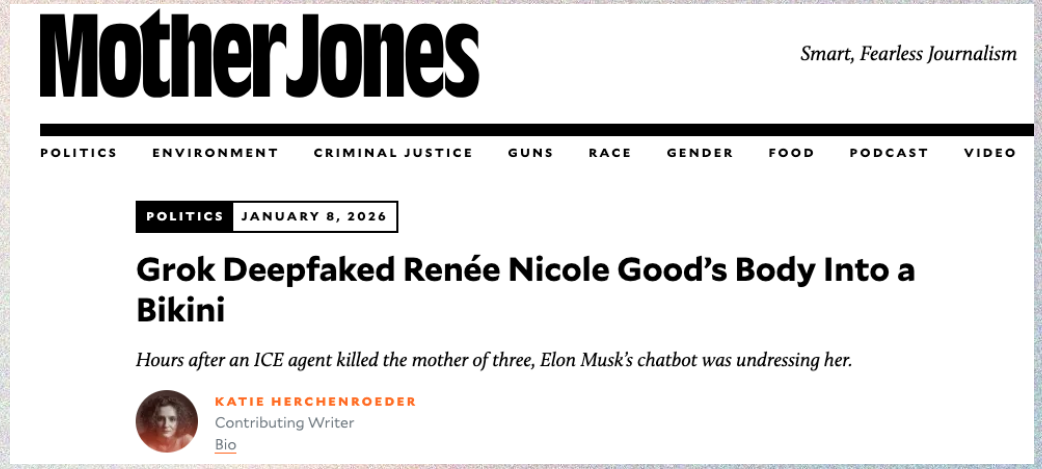
MIS/DISINFORMATION

- AI created mis/disinformation (images, video, audio, text)
- Bots that spread information, engage in and promote sexist and misogynistic content
- Bots that divide communities
- Algorithms promote divisive content
- Manosphere/misogynistic promoted
- Creating fake content about a person to cause them harm

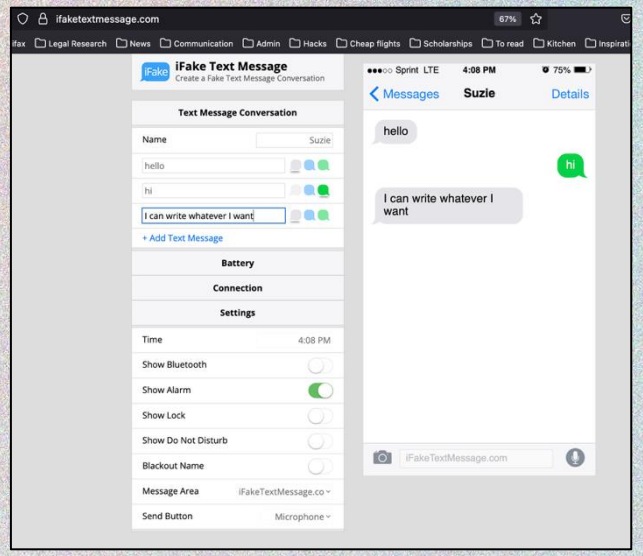


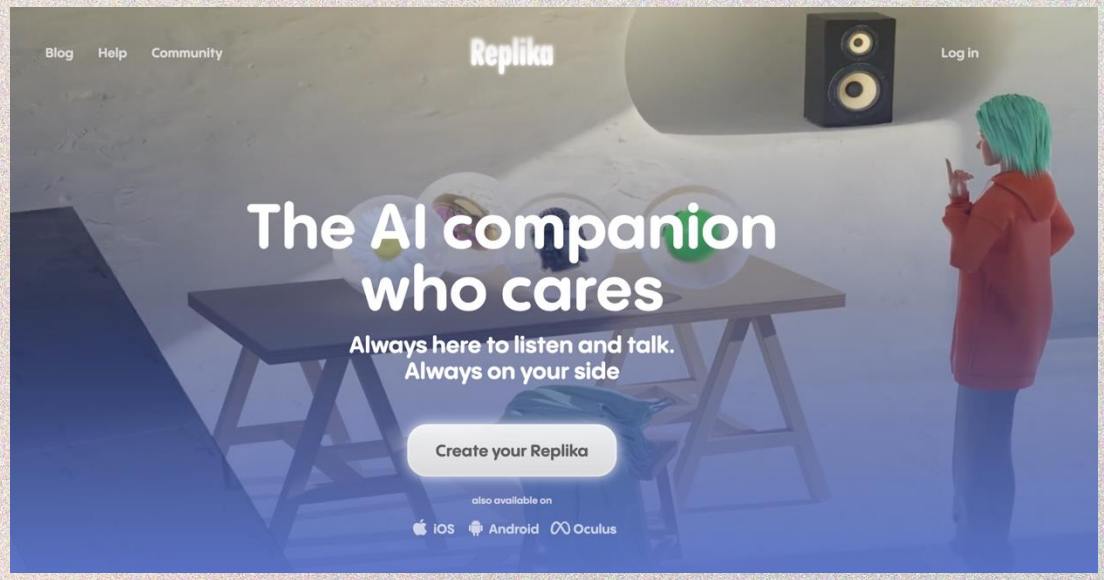


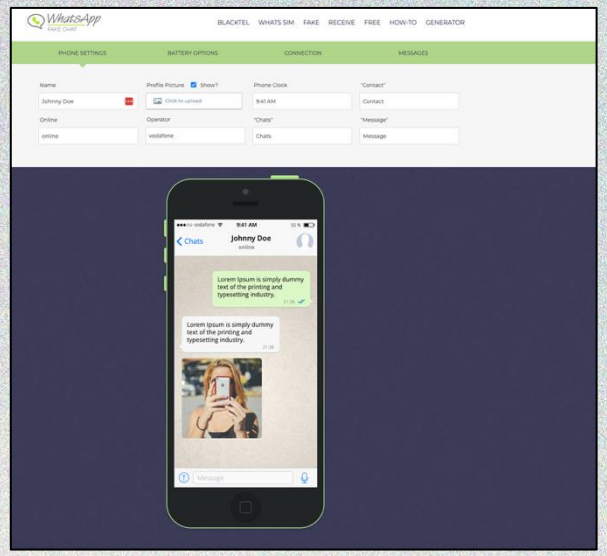


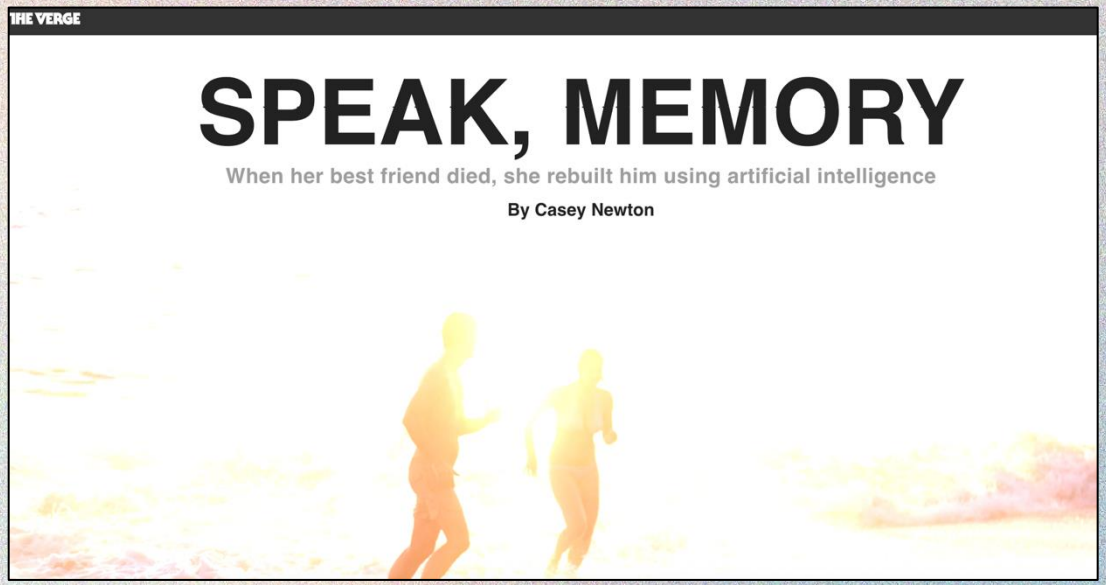


TEXT SPOOFING: AI MIMICS STYLE

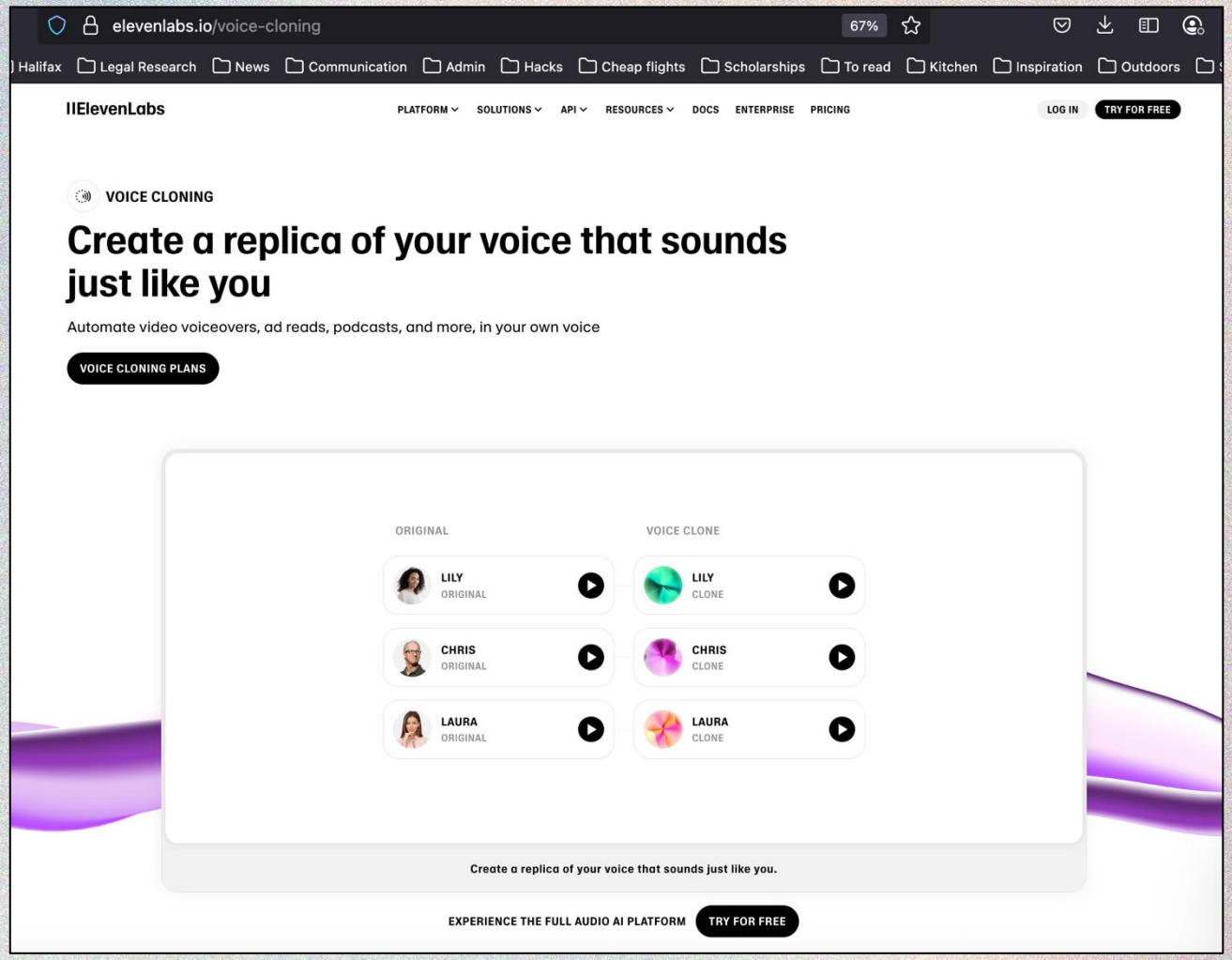




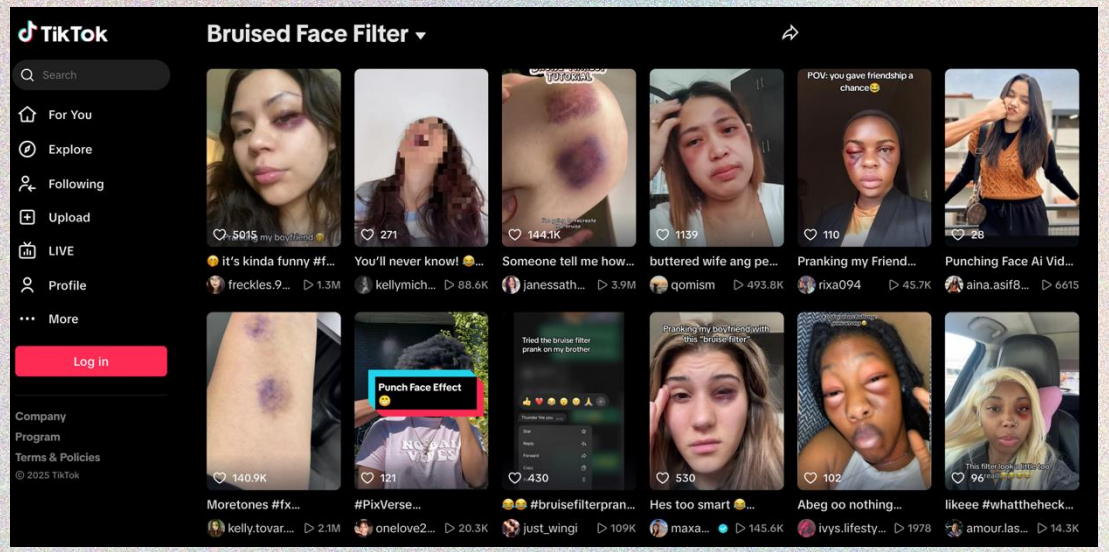


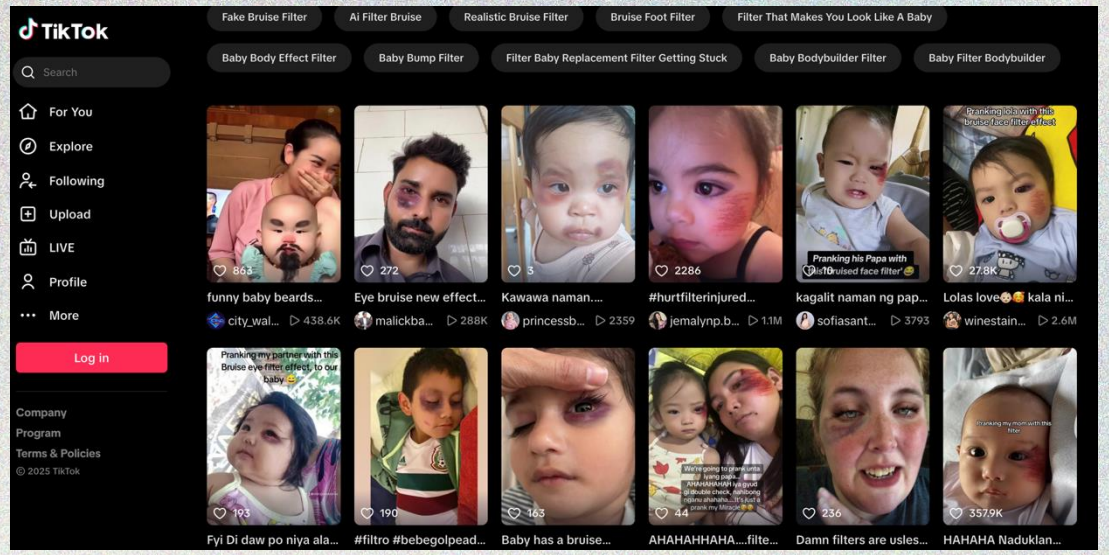


VOICE CLONING

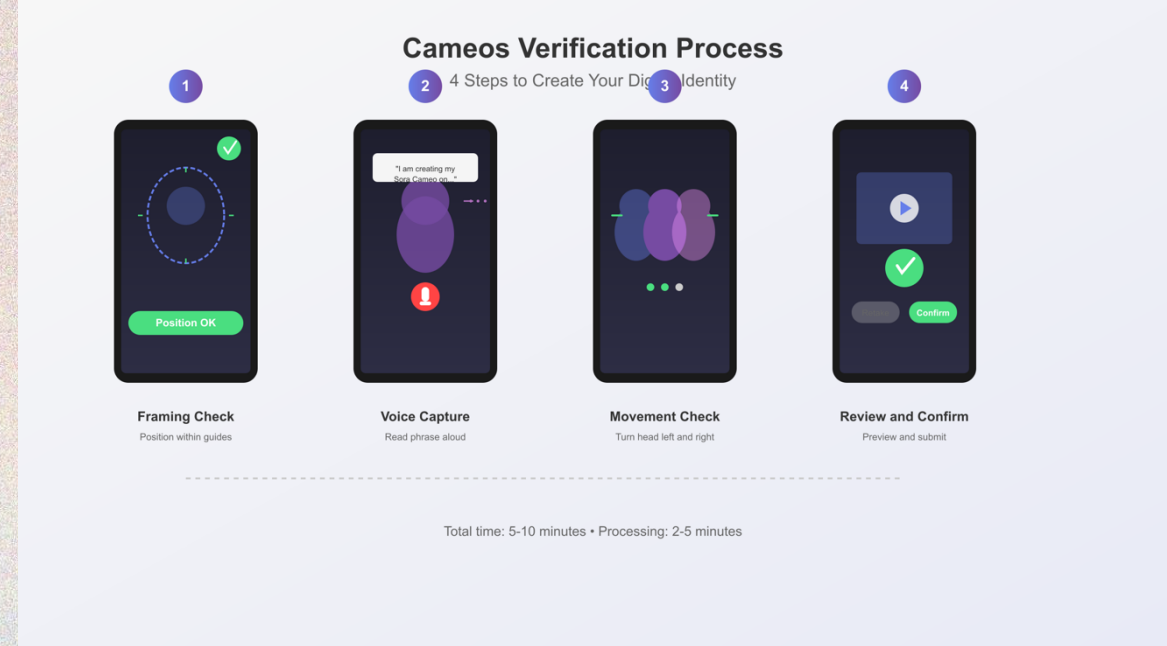


FILTERS AND PHOTO EDITING





SORA 2 AND CAMEOS



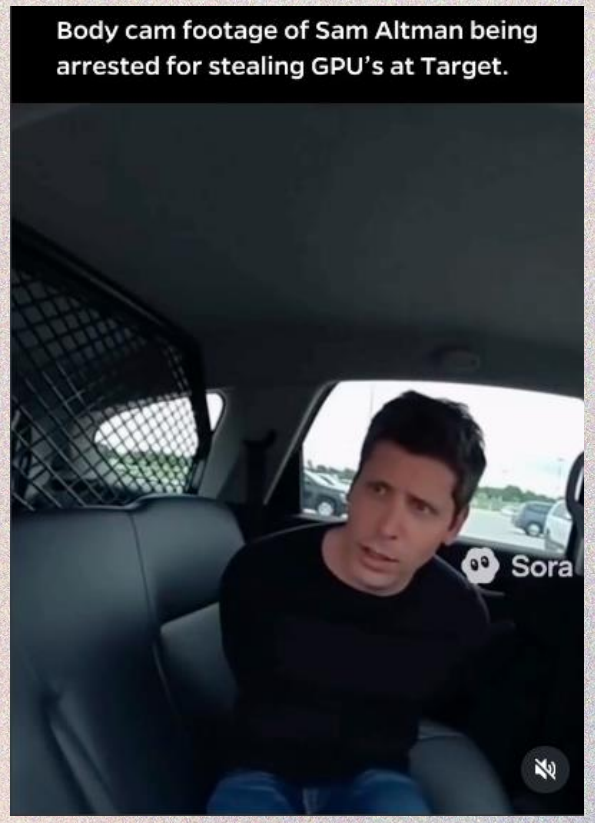
SORA 2 AND CAMEOS

Update who can use your cameo

You can choose who is allowed to feature your cameo in their videos:

- **Only me** — Only you can use your cameo.
- **People I approve** — When you choose this option, you can select specific users that have permission to use your cameo. You can update this list at any time by selecting this option again.
- **Mutuals** — People you follow **and** who follow you back.
- **Everyone** — Anyone can feature your cameo (subject to platform rules).

Please note that changes apply going forward but you always have the option to delete content that uses your cameo.
Teen accounts are restricted to either "only me" or "people I approve" privacy settings.



https://help.openai.com/en/articles/12435986-generating-content-with-cameos
https://www.nytimes.com/2025/10/03/podcasts/sora-and-the-infinite-slop-feeds-chatgpt-goes-to-therapy-hot-mess-express.html
https://www.404media.co/podcast-the-final-boss-of-ai-slop/

Synthetic CSAM

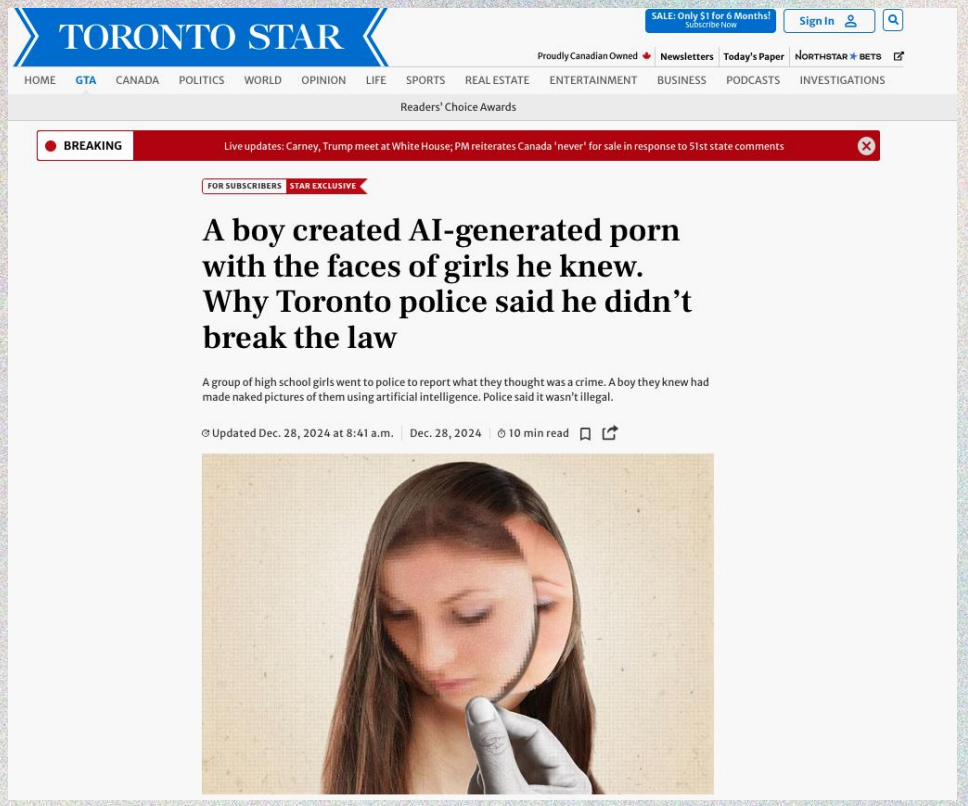
R c Larouche, 2023 QCCQ 1853

- Large collection of child pornography
- Including sexual deepfakes of children
- Makes hashing difficult
- Possessing, making, distributing
- Increasing images of known victims

R v Legault, 2024 BCPC 29

- Catfishing girls he met as a youth pastor
- Created and sent sexual deepnudes of the girls
- Making, possessing

PRIVATE USE EXCEPTION



TORONTO STAR

SALE: Only $1 for 6 Months! Subscribe Now | Sign In

Proudly Canadian Owned | Newsletters | Today's Paper | NORTHSTAR BETS

HOME GTA CANADA POLITICS WORLD OPINION LIFE SPORTS REAL ESTATE ENTERTAINMENT BUSINESS PODCASTS INVESTIGATIONS

Readers' Choice Awards

BREAKING Live updates: Carney, Trump meet at White House; PM reiterates Canada 'never' for sale in response to 51st state comments

FOR SUBSCRIBERS STAR EXCLUSIVE

A boy created AI-generated porn with the faces of girls he knew. Why Toronto police said he didn't break the law

A group of high school girls went to police to report what they thought was a crime. A boy they knew had made naked pictures of them using artificial intelligence. Police said it wasn't illegal.

Updated Dec. 28, 2024 at 8:41 a.m. | Dec. 28, 2024 | 10 min read

- Police told teen girls who had their images deepfaked that they would not fit under the Criminal Code's Child Pornography provision because the boys creation of the images fell into the private use exception from *R v Sharpe*

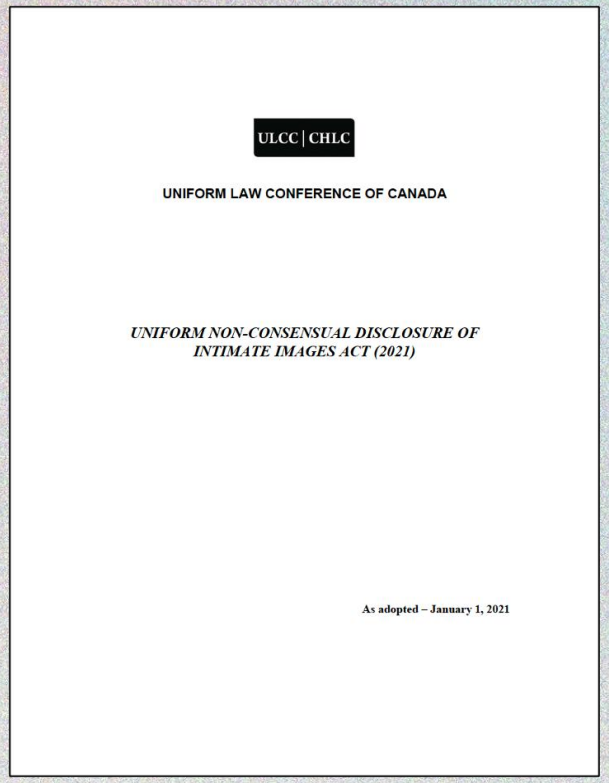
- *"When the investigator told them there was no proof of distribution and the boy made the photos for 'private use,' some of the girls said the accused had shown the pictures to a few other boys they knew."*

- Should deepfakes that are not distributed and only held for private use be protected by this exception?

PRIVATE USE EXCEPTION

- *R v TW*, 2014 ONSC 4532
  - Not created solely by the accused
  - Used images taken from elsewhere and complied them in a journal with other material advocating for child sexual abuse (some could be categorized as child pornography)
  - Private use exception did not apply as “the accused’s journal consists of pornographic images that the accused secured from some external source, such as a book, magazine or internet website.”
  - This content “(a) reinforce the cognitive distortion that pedophilia is a normal and acceptable sexual preference; and (b) fuel the sexual fantasies of pedophiles and encourage them to act upon those fantasies.”

CIVIL INTIMATE IMAGES

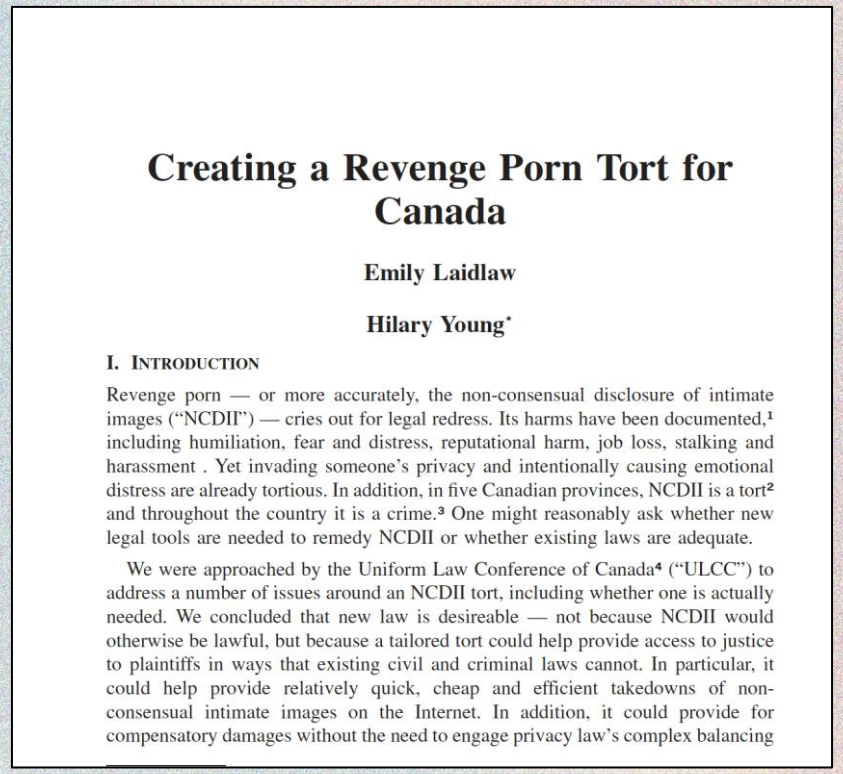


ULCC | CHLC

UNIFORM LAW CONFERENCE OF CANADA

UNIFORM NON-CONSENSUAL DISCLOSURE OF INTIMATE IMAGES ACT (2021)

As adopted – January 1, 2021



Creating a Revenge Porn Tort for Canada

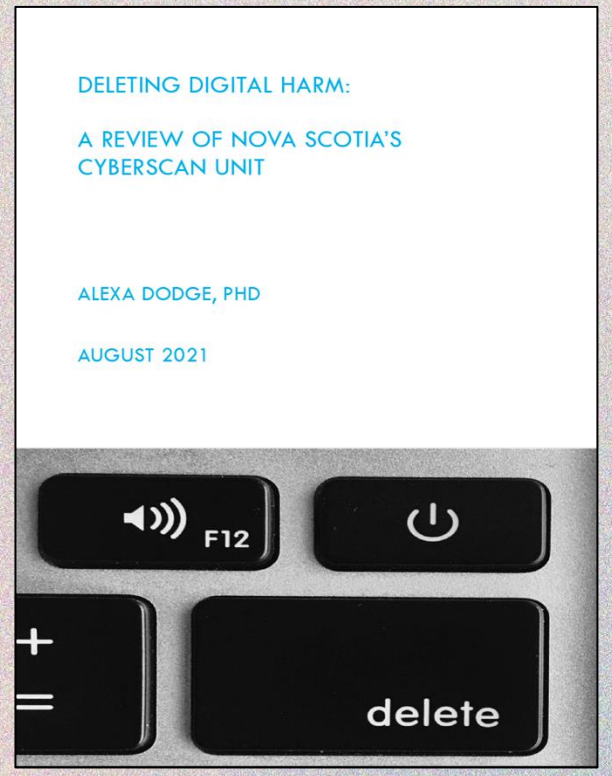
Emily Laidlaw

Hilary Young*

I. Introduction

Revenge porn — or more accurately, the non-consensual disclosure of intimate images ("NCDII") — cries out for legal redress. Its harms have been documented,[1] including humiliation, fear and distress, reputational harm, job loss, stalking and harassment . Yet invading someone's privacy and intentionally causing emotional distress are already tortious. In addition, in five Canadian provinces, NCDII is a tort[2] and throughout the country it is a crime.[3] One might reasonably ask whether new legal tools are needed to remedy NCDII or whether existing laws are adequate.

We were approached by the Uniform Law Conference of Canada[4] ("ULCC") to address a number of issues around an NCDII tort, including whether one is actually needed. We concluded that new law is desireable — not because NCDII would otherwise be lawful, but because a tailored tort could help provide access to justice to plaintiffs in ways that existing civil and criminal laws cannot. In particular, it could help provide relatively quick, cheap and efficient takedowns of non-consensual intimate images on the Internet. In addition, it could provide for compensatory damages without the need to engage privacy law's complex balancing



DELETING DIGITAL HARM:

A REVIEW OF NOVA SCOTIA'S CYBERSCAN UNIT

ALEXA DODGE, PHD

AUGUST 2021

CIVIL INTIMATE IMAGES

Alberta: *Protecting Victims of Non-consensual Distribution of Intimate Images Act*, RSA 2017, c P-26.9.

British Columbia: *Intimate Images Protection Act*, SBC 2023, c 11.

Manitoba: *The Intimate Image Protection Act*, CCSM c 187.

Newfoundland and Labrador: *Intimate Images Protection Act*, SNL 2018, c I-22.

Nova Scotia: *Intimate Images and Cyber-protection Act*, SNS 2017, c 7.

New Brunswick: *Intimate Images Unlawful Distribution Act*, SNB 2022, c 1.

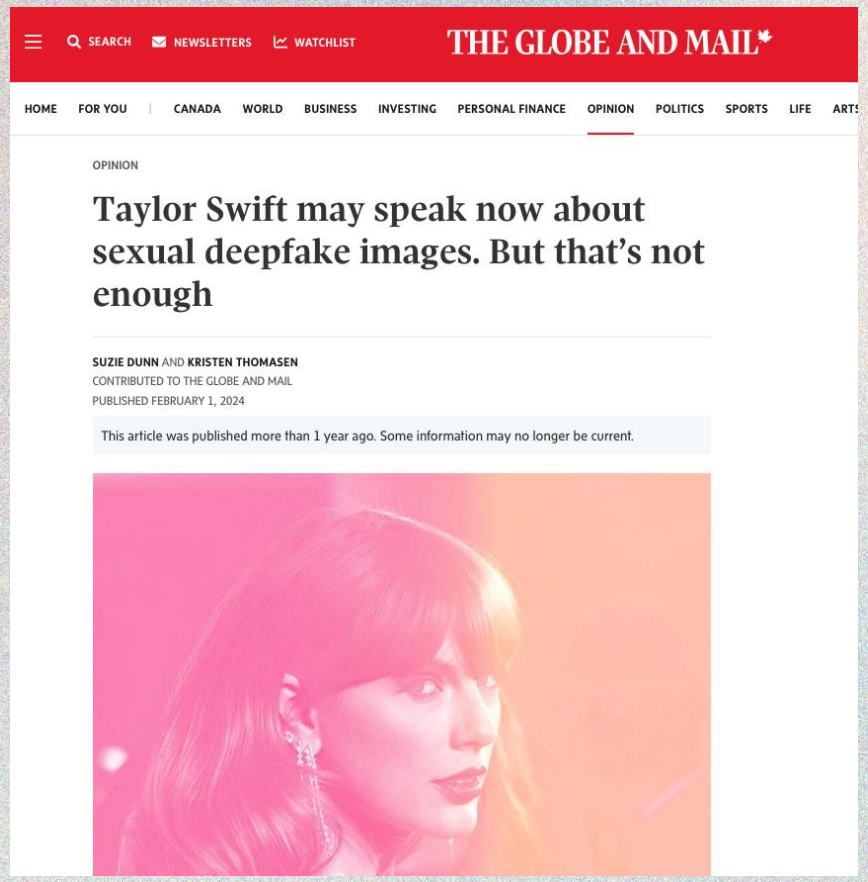
Price Edward Island: *Intimate Images Protection Act*, RSPEI 1988, c I-9.1.

Quebec*, Act to Counter Non-consensual Sharing of Intimate Images*

Saskatchewan: *The Privacy Act,* RSC, 1985, C P-24, Part 2.

Provinces and Territories without NCDII Statutes: Ontario, Yukon, NWT, Nunavut

CIVIL INTIMATE IMAGES



Manitoba: Fake Intimate images

any type of visual recording

a) that, in a reasonably convincing manner, falsely depicts an identifiable person

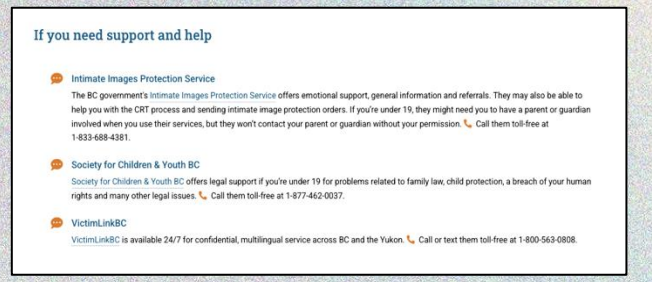
(i) as being nude or exposing their genital organs, anal region or breasts, or

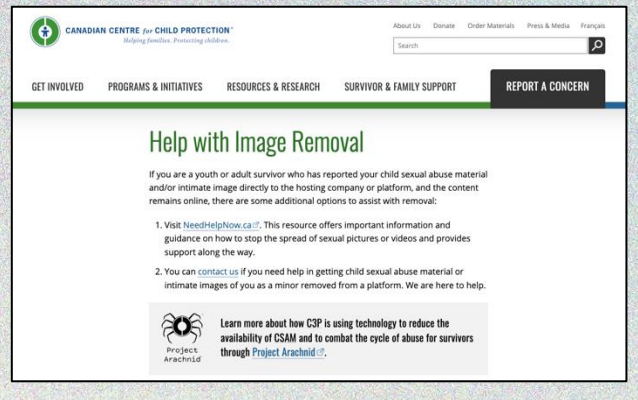
(ii) engaging in explicit sexual activity;

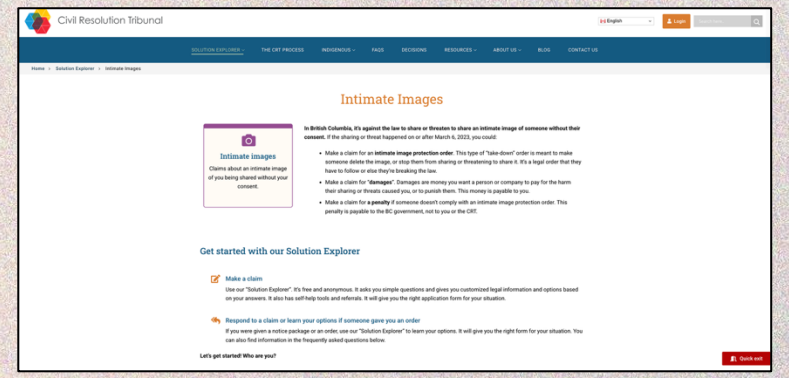
b) that is created through the use of software, machine learning, artificial intelligence or other means, including by modifying, manipulating or altering an authentic visual representation; and

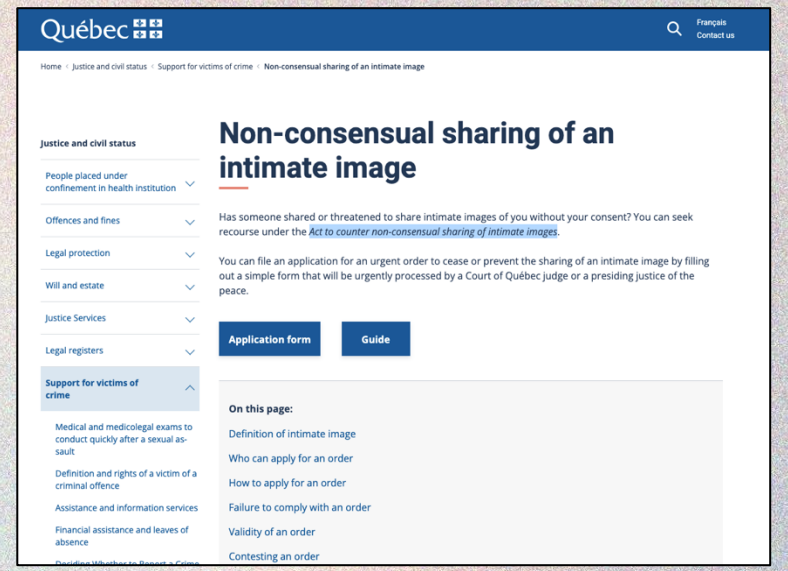
c) in respect of which it is reasonable to suspect that the person depicted in the image would not consent to the recording being made or distributed to others.

STATUTORY BODIES





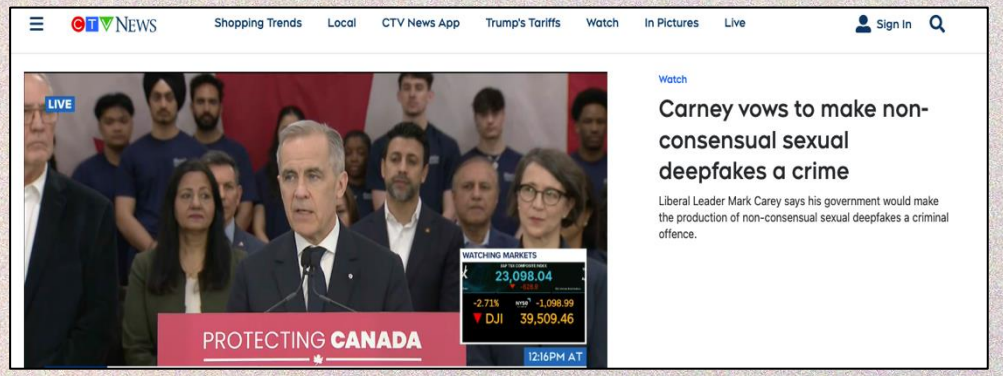




BILL C-16

Bill C-16
Definition of intimate image
(2) In this section, intimate image means
(a) a visual recording of a person made by any means including a photographic, film or video recording, (i) in which the **person is nude, is exposing Insertion start their sexual Insertion end organs or is engaged in explicit sexual activity**, (ii) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy, and (iii) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed;

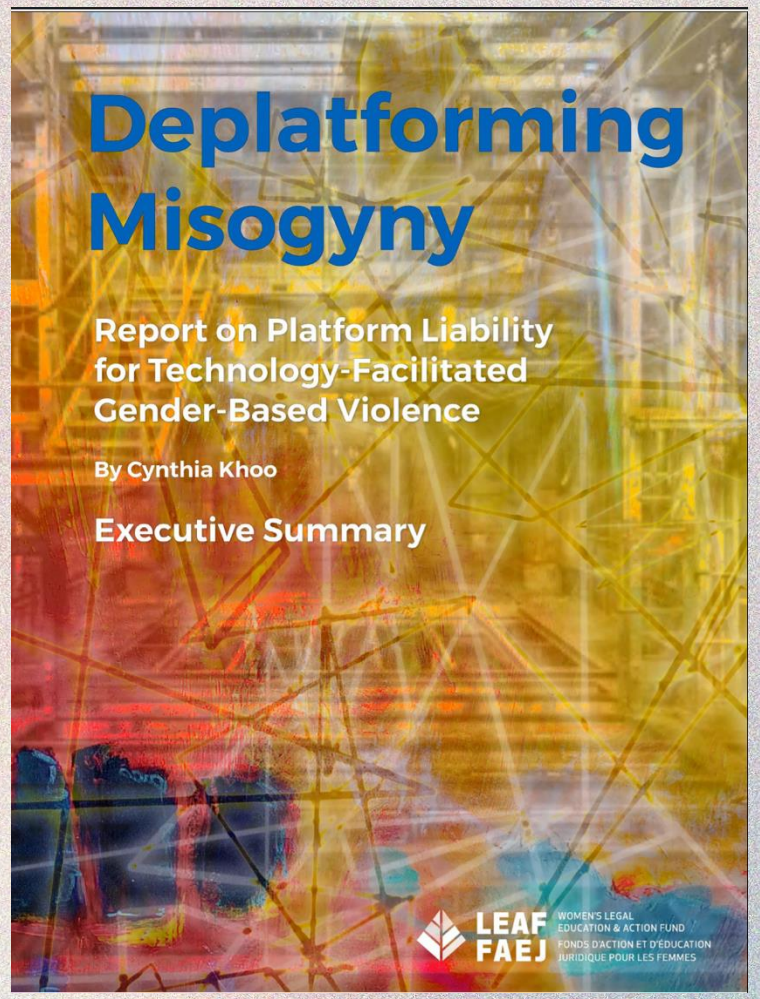
(b) a visual representation that is made by any electronic or mechanical means and that shows an identifiable person who is depicted as nude, as exposing their sexual organs or as engaged in explicit sexual activity, if the depiction is likely to be mistaken for a visual recording of that person.



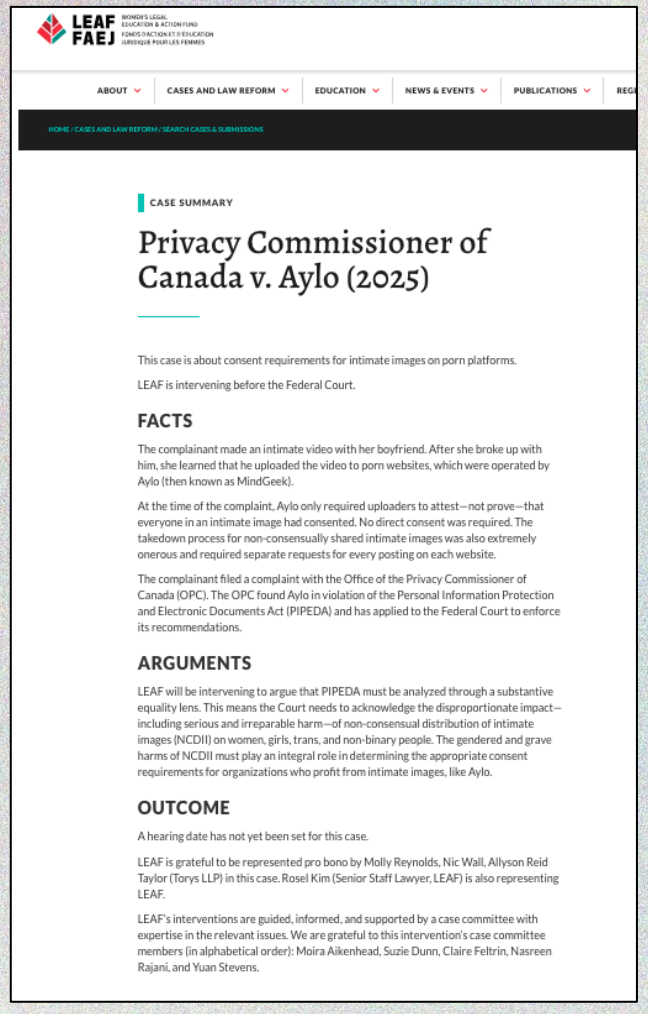
CONTENT MODERATION

Content Moderation

- Proposed Online Harms Bill C-63 (Died upon proroguing of Parliament)
  - Content moderation of social media websites
  - Obligations to mitigate harms
  - Obligations to remove NCDII and CSAM, including deepfakes, within 24 hours



PRIVACY COMMISSIONER



LEAF FAEJ

ABOUT | CASES AND LAW REFORM | EDUCATION | NEWS & EVENTS | PUBLICATIONS

HOME / CASES AND LAW REFORM / SEARCH CASES & SUBMISSIONS

CASE SUMMARY

Privacy Commissioner of Canada v. Aylo (2025)

This case is about consent requirements for intimate images on porn platforms.

LEAF is intervening before the Federal Court.

FACTS

The complainant made an intimate video with her boyfriend. After she broke up with him, she learned that he uploaded the video to porn websites, which were operated by Aylo (then known as MindGeek).

At the time of the complaint, Aylo only required uploaders to attest—not prove—that everyone in an intimate image had consented. No direct consent was required. The takedown process for non-consensually shared intimate images was also extremely onerous and required separate requests for every posting on each website.

The complainant filed a complaint with the Office of the Privacy Commissioner of Canada (OPC). The OPC found Aylo in violation of the Personal Information Protection and Electronic Documents Act (PIPEDA) and has applied to the Federal Court to enforce its recommendations.

ARGUMENTS

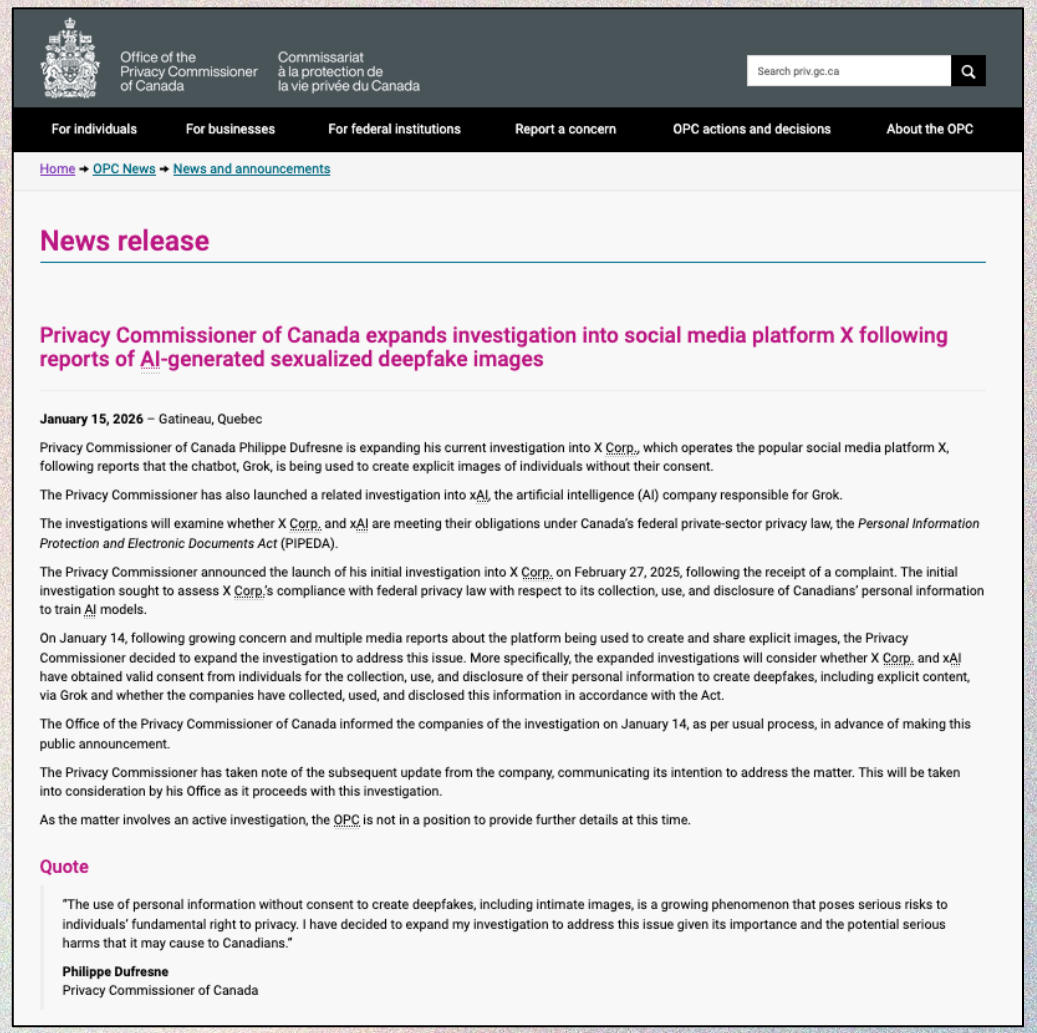
LEAF will be intervening to argue that PIPEDA must be analyzed through a substantive equality lens. This means the Court needs to acknowledge the disproportionate impact—including serious and irreparable harm—of non-consensual distribution of intimate images (NCDII) on women, girls, trans, and non-binary people. The gendered and grave harms of NCDII must play an integral role in determining the appropriate consent requirements for organizations who profit from intimate images, like Aylo.

OUTCOME

A hearing date has not yet been set for this case.

LEAF is grateful to be represented pro bono by Molly Reynolds, Nic Wall, Allyson Reid Taylor (Torys LLP) in this case. Rosel Kim (Senior Staff Lawyer, LEAF) is also representing LEAF.

LEAF's interventions are guided, informed, and supported by a case committee with expertise in the relevant issues. We are grateful to this intervention's case committee members (in alphabetical order): Moira Aikenhead, Suzie Dunn, Claire Feltrin, Nasreen Rajani, and Yuan Stevens.



Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Search priv.gc.ca

For individuals | For businesses | For federal institutions | Report a concern | OPC actions and decisions | About the OPC

Home ➜ OPC News ➜ News and announcements

News release

Privacy Commissioner of Canada expands investigation into social media platform X following reports of AI-generated sexualized deepfake images

January 15, 2026 – Gatineau, Quebec

Privacy Commissioner of Canada Philippe Dufresne is expanding his current investigation into X Corp., which operates the popular social media platform X, following reports that the chatbot, Grok, is being used to create explicit images of individuals without their consent.

The Privacy Commissioner has also launched a related investigation into xAI, the artificial intelligence (AI) company responsible for Grok.

The investigations will examine whether X Corp. and xAI are meeting their obligations under Canada's federal private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The Privacy Commissioner announced the launch of his initial investigation into X Corp. on February 27, 2025, following the receipt of a complaint. The initial investigation sought to assess X Corp.'s compliance with federal privacy law with respect to its collection, use, and disclosure of Canadians' personal information to train AI models.

On January 14, following growing concern and multiple media reports about the platform being used to create and share explicit images, the Privacy Commissioner decided to expand the investigation to address this issue. More specifically, the expanded investigations will consider whether X Corp. and xAI have obtained valid consent from individuals for the collection, use, and disclosure of their personal information to create deepfakes, including explicit content, via Grok and whether the companies have collected, used, and disclosed this information in accordance with the Act.

The Office of the Privacy Commissioner of Canada informed the companies of the investigation on January 14, as per usual process, in advance of making this public announcement.

The Privacy Commissioner has taken note of the subsequent update from the company, communicating its intention to address the matter. This will be taken into consideration by his Office as it proceeds with this investigation.

As the matter involves an active investigation, the OPC is not in a position to provide further details at this time.

Quote

> "The use of personal information without consent to create deepfakes, including intimate images, is a growing phenomenon that poses serious risks to individuals' fundamental right to privacy. I have decided to expand my investigation to address this issue given its importance and the potential serious harms that it may cause to Canadians."
>
> **Philippe Dufresne**
> Privacy Commissioner of Canada

LIAR'S DIVIDEND: CLAIMING REAL EVIDENCE IS SYNTHETIC

R v Vitellaro, 2025 ONCJ 200

- Claimed cell video evidence was "CGI deepfake"
- Video caught on driver's dashcam
- Compared videos

R v Cheng, 2025 ONCJ 252

- Failing to comply with condition of bail (family separation involved)
- Home surveillance video showed he attended residence, gaps in video
- Tried to argue video was fake or altered
- Looked to clothing, functionality of recording device
- [para 7] "…the emergence of "deepfake" evidence and the ability to manipulate electronic records means this court must carefully consider the weight to be given these exhibits."

Suzie Dunn
Assistant Professor
Director of the Law and Technology Institute, Schulich School of Law, Dalhousie University
Find my research here

www.suziedunn.com
www.diydigitalsafety.ca

suzie.dunn@dal.ca

THANK YOU!