

Matt Burgess, Deepfake Porn Is Out of Control, Wired (Oct. 16, 2023)

Google's and Microsoft's search engines have a problem with deepfake porn videos. Since [deepfakes](#) emerged half a decade ago, the technology has consistently been used to abuse and harass women—using machine learning to morph someone's head into pornography without their permission. Now the number of nonconsensual deepfake porn videos is growing at an exponential rate, fueled by the advancement of [AI](#) technologies and an expanding deepfake ecosystem.

A new analysis of nonconsensual deepfake porn videos, conducted by an independent researcher and shared with WIRED, shows how pervasive the videos have become. At least 244,625 videos have been uploaded to the top 35 websites set up either exclusively or partially to host deepfake porn videos in the past seven years, according to the researcher, who requested anonymity to avoid being targeted online.

Over the first nine months of this year, 113,000 videos were uploaded to the websites—a 54 percent increase on the 73,000 videos uploaded in all of 2022. By the end of this year, the analysis forecasts, more videos will have been produced in 2023 than the total number of every other year combined.

These startling figures are just a snapshot of how colossal the issues with nonconsensual deepfakes has become—the full scale of the problem is much larger and encompasses other types of manipulated imagery. A whole industry of deepfake abuse, which predominantly targets women and is produced without people's consent or knowledge, has emerged in recent years. Face-swapping apps that work on still images and apps where clothes can be “stripped off a person” in a photo with [just a few clicks](#) are also highly prominent. There are likely millions of images being created with these apps.

“This is something that targets everyday people, everyday high school students, everyday adults—it's become a daily occurrence,” says Sophie Maddocks, who conducts research on digital rights and cyber-sexual violence at the University of Pennsylvania. “It would make a lot of difference if we were able to make these technologies harder to access. It shouldn't take two seconds to potentially incite a sex crime.”

The new research highlights 35 different websites, which exist to exclusively host deepfake pornography videos or incorporate the videos alongside other adult material. (It does not encompass videos posted on social media, those shared privately, or manipulated photos.) WIRED is not naming or directly linking to the websites, so as not to further increase their visibility. The researcher scraped the websites to analyze the number and duration of deepfake videos, and they looked at how people find the websites using the analytics service SimilarWeb.

Many of the websites make it clear they host or spread deepfake porn videos—often featuring the word *deepfakes* or derivatives of it in their name. The top two websites contain 44,000 videos each, while five others host more than 10,000 deepfake videos. Most of them have several thousand videos, while some only list a few hundred. Some videos the researcher analyzed have been watched millions of times.

The research also identified an additional 300 general pornography websites that incorporate nonconsensual deepfake pornography in some way. The researcher says “leak” websites and websites that exist to repost people’s social media pictures are also incorporating deepfake images. One website dealing in photographs claims it has “undressed” people in 350,000 photos.

Measuring the full scale of deepfake videos and images online is incredibly difficult. Tracking where the content is shared on social media is challenging, while abusive content is also shared in private messaging groups or closed channels, often by people known to the victims. In September, more than 20 girls aged 11 to 17 came forward in the Spanish town of Almendralejo after AI tools were used to generate naked photos of them [without their knowledge](#).

“There has been significant growth in the availability of AI tools for creating deepfake nonconsensual pornographic imagery, and an increase in demand for this type of content on pornography platforms and illicit online networks,” says Asher Flynn, an associate professor at Monash University, Australia, who focuses on AI and technology-facilitated abuse. This is only likely to increase with new generative AI tools.

The gateway to many of the websites and tools to create deepfake videos or images is through search. Millions of people are directed to the websites analyzed by the researcher, with 50 to 80 percent of people finding their way to the websites via search. Finding deepfake videos through search is trivial and does not require a person to have any special knowledge about what to search for.

The issue is global. Using a VPN, the researcher tested Google searches in Canada, Germany, Japan, the US, Brazil, South Africa, and Australia. In all the tests, deepfake websites were prominently displayed in search results. Celebrities, streamers, and content creators are often targeted in the videos. Maddocks says the spread of deepfakes has become “endemic” and is what many researchers first feared when the first deepfake videos rose to [prominence in December 2017](#).

Since the tools needed to create deepfake videos emerged, they’ve become easier to use, and the quality of the videos being produced has improved. The wave of image-generation tools also offers the potential for higher-quality abusive images and, eventually, video to be created. And five years after the first deepfakes started to appear, the [first laws are just emerging](#) that criminalize the sharing of faked images.

The proliferation of these deepfake apps combined with a greater reliance on digital communications in the Covid-19 era and a “failure of laws and policies to keep pace” has created a “perfect storm,” Flynn says.

Experts say that alongside new laws, better education about the technologies is needed, as well as measures to stop the spread of tools created to cause harm. This includes action by firms that host the websites and also search engines, including Google and Microsoft’s Bing. Currently, Digital Millennium Copyright Act (DMCA) complaints are the primary legal mechanism that women have to get videos removed from websites.

Henry Ajder, a deepfake and generative AI expert who has [monitored the spread of the technologies](#), says adding more “friction” to the process of people finding deepfake porn videos, apps to change people’s faces, and tools that specifically allow the creation of nonconsensual images can reduce the spread. “It’s about trying to make it as hard as possible for someone to find,” he says. This could be search engines down-ranking results for harmful websites or internet service providers blocking sites, he says. “It’s hard to feel really optimistic, given the volume and scale of these operations, and the need for platforms—which historically have not taken these issues seriously—to suddenly do so,” Ajder says.

“Like any search engine, Google indexes content that exists on the web, but we actively design our ranking systems to avoid shocking people with unexpected harmful or explicit content they don’t want to see,” says Google spokesperson Ned Adriaance, pointing to its [page on when it removes search results](#). Google’s support pages say it is possible for people to request that “involuntary fake pornography” be removed. Its [removal form](#) requires people to manually submit URLs and the search terms that were used to find the content. “As this space evolves, we’re actively working to add more safeguards to help protect people, based on systems we’ve built for other types of nonconsensual explicit imagery,” Adriaance says.

Courtney Gregoire, chief digital safety officer at Microsoft, says it does not allow deepfakes, and they can be reported through its [web forms](#). “The distribution of nonconsensual intimate imagery (NCII) is a gross violation of personal privacy and dignity with devastating effects for victims,” Gregoire says. “Microsoft prohibits NCII on our platforms and services, including the soliciting of NCII or advocating for the production or redistribution of intimate imagery without a victim’s consent.”

While the number of videos and pictures continues to skyrocket, the impact on victims can be long-lasting. “Gender-based online harassment is having an enormous chilling effect on free speech for women,” Maddocks says. As [reported by WIRED](#), female Twitch streamers targeted by deepfakes have detailed feeling violated, being exposed to more harassment, and losing time, and some said the nonconsensual content found its way to family members.

Flynn, the Monash University professor, says her research has found “high rates” of mental health concerns—such as anxiety, depression, self-injury, and suicide—as a result of digital abuse. “The potential impacts on a person’s mental and physical health, as well as impacts on their employment, family, and social lives can be immense,” Flynn says, “regardless of whether the image is deepfaked or ‘real.’”