She thought a dark moment in her past was forgotten. Then she scanned her face online

By Rachel Metz, CNN Business

Updated 12:18 PM ET, Tue May 24, 2022

(CNN Business) — Cher Scarlett, a software engineer, has a history of being misidentified by face-scanning technology, including one instance that may have surfaced a distant ancestor in a photo. So when she was introduced to an online facial-recognition tool she hadn't heard of, she wanted to see whether it would mistake photos of her mom or daughter for her.

On February 1, Scarlett uploaded some images of her teenage daughter and her mom to PimEyes, a facial-recognition website meant to be used to find pictures of yourself from around the web — ostensibly to help stamp out issues such as revenge porn and identity theft. She didn't get any images of herself in return — pictures of her daughter yielded other kids, she said, while one of her mom led to some pictures of her mother, plus images of other, similar-looking women.

She decided to try something else. Scarlett next uploaded a couple pictures of herself, curious if they would lead to pictures of her relatives. They didn't, but the results stunned her anyway: tucked under some recent images of herself and mistaken matches showing photos of Britney Spears and the pop star's sister, Jamie Lynn, were pictures of a younger version of Scarlett. They were pictures of a dark time she didn't totally remember —a time at age 19 when, she said, she traveled to New York and was coerced into engaging in humiliating and, at times, violent sexual acts on camera.

"I'm looking at these pictures, and all I can think is that somebody has photoshopped my face onto porn," Scarlett told CNN Business in an interview.

Scarlett, who is known for being a former Apple employee who founded the worker organizing movement known as #AppleToo, has been open online and in the media about her life and struggles, which she has said include experiencing sexual abuse as a child, dropping out of high school, battling addiction, and having nude pictures of herself shared online without her consent.

What happened to her in New York in 2005 was so traumatic that she tried to take her own life in the weeks that followed, she said, and in 2018 she began going by the last name Scarlett (she officially changed her name in December 2021).

Cher Scarlett, a software engineer, told CNN Business in an interview: "I'm looking at these pictures, and all I can think is that somebody has photoshopped my face onto porn."

She's worked hard to overcome past trauma. Based in Kirkland, Washington, she's spent years working as a software engineer. She's raising her daughter, and she's a recovering drug addict. Since leaving Apple in late 2021 — she has pending complaints against Apple that are being investigated by the National Labor Relations Board (Apple did not respond to a request for comment) — she began a job as a senior software engineer at video game developer ControlZee in March.

But with a few clicks of a mouse, PimEyes brought back a real-life nightmare that occurred nearly two decades ago. She has since tried and failed to get all of the explicit photos removed from PimEyes' search results, despite the site saying it would scrub images of Scarlett from results. As of this week, sexually explicit images of Scarlett could still be found via PimEyes.

Giorgi Gobronidze, who identified himself to CNN Business as the current owner and director of PimEyes (he said he bought the company from its previous owners in December), said he wishes nobody would experience what Scarlett went through, which he acknowledged as "very, very painful."

"However, just simply saying, 'I don't want to see images' or 'I don't want to see the problem' doesn't make the problem disappear," he said. "The problem isn't that there is a search engine that can find these photos; the problem is there are the photos and there are people who actually uploaded and did it on purpose."

It's true that the discovery of unknown images may be useful for some people who are attempting to stamp out such pictures of themselves online. But Scarlett's saga starkly shows how easily facial-recognition technology, which is now available to anyone with internet access, can lead to unexpected harms that may be impossible to undo. The technology has become increasingly common across the United States in the past several years, and there are no current federal rules regulating its use. Yet it has been blasted by privacy and digital rights groups over privacy and racial bias issues and other real and potential dangers.

More people will "undoubtedly" have experiences like Scarlett's, said Woodrow Hartzog, a professor of law and computer science at Northeastern University. "And we know from experience that the people who will suffer first and suffer the hardest are women and people of color and other marginalized communities for whom facial-recognition technology serves as a tool of control over."

As Scarlett put it, "I can't imagine the horrible pain of having that part of my life exposed not by me -— by somebody else."

"You may find this interesting"

Scarlett's discovery of the stash of photos on PimEyes was my fault.

I've long been familiar with her work as a labor activist, and follow her on Twitter. Because I write often about facial-recognition software, I contacted her after she posted a confounding tweet in late January related to an experience she had on Facebook in October 2021. Scarlett had been tagged in an old-looking black-and-white picture of a woman and man — a photo that had been posted to Facebook by a friend of a friend, to whom she said she is distantly related.

She said at the time she had been "auto-tagged" via Facebook's facial-recognition software, which was disabled after the photo had been posted; she now believes the tag was a suggestion enabled by the software.

Stranger still: Some sleuthing on Ancestry.com led her to believe the woman in the photo was her great-great-great grandmother.

(Facebook said it never automatically tagged users in images — prior to turning off the facial-recognition feature it could, however, suggest that a user be tagged in an image if that user had the facial-recognition setting turned on, and would notify a user if they appeared in an image on Facebook but hadn't been tagged.)

Scarlett and I talked, via Twitter's private messages, about the strangeness of this experience and the impacts of facial-recognition software.

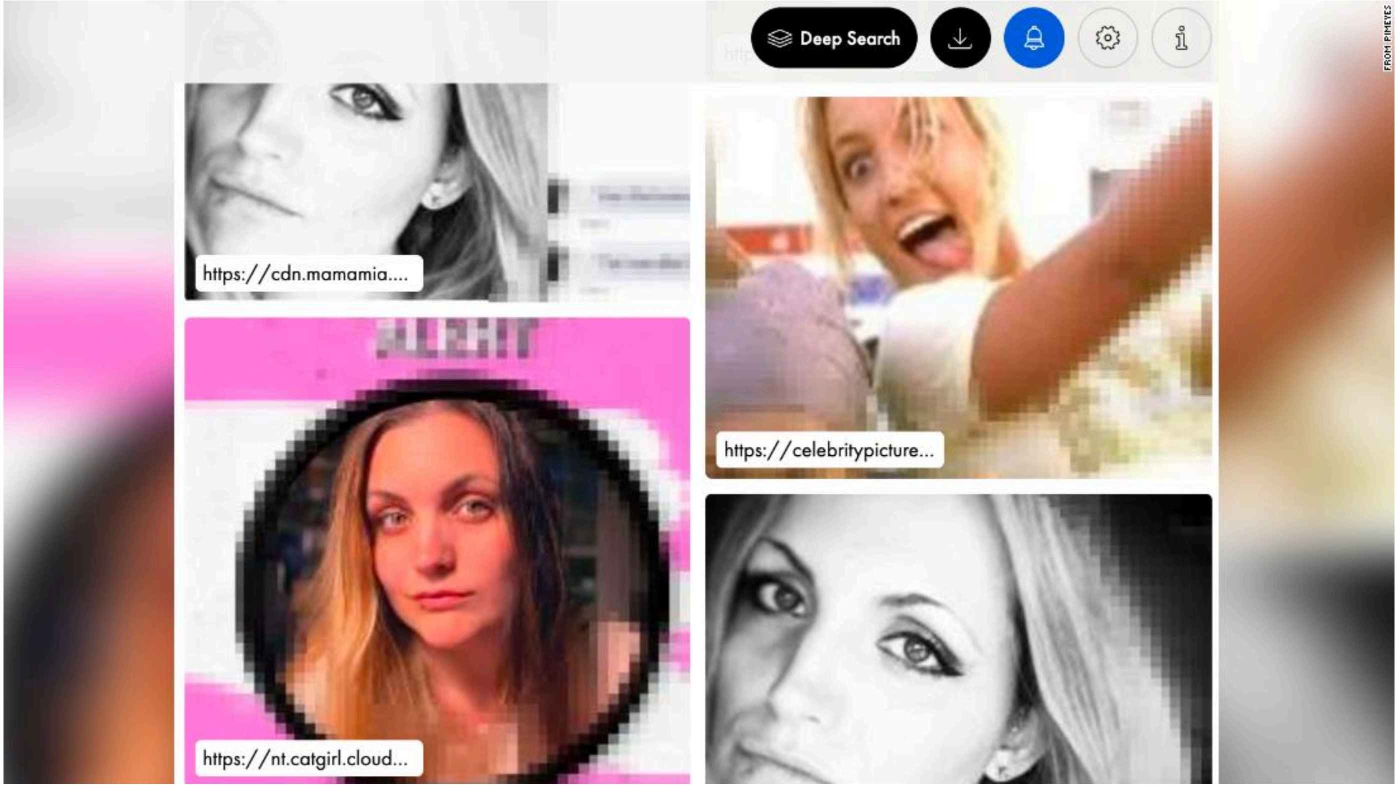
That's when I sent her a link to a story I had written in May 2021 about a website called PimEyes. Though the website instructs users to search for themselves, it doesn't stop them from uploading photos of anyone. And while it doesn't explicitly identify anyone by name, as CNN Business discovered by using the site, that information may be just clicks away from the images PimEyes pulls up.

Its images come from a range of websites, including company, media and pornography sites — the last of which PimEyes told CNN Business in 2021 that it includes so people can search online for any revenge porn in which they may unknowingly appear. PimEyes says it doesn't scrape images from social media.

"You may find this interesting," I wrote, introducing my article.

Minutes later, Scarlett told me she had paid $30 for PimEyes' cheapest monthly service. (PimEyes shows users a free, somewhat blurred preview of each image that its facial-recognition software determines is likely to include the same person as in the photo that the user initially uploaded; you have to pay a fee to click through to go to the websites where the images appear.)

Shortly after that, she sent me a message: "oh no."



A screenshot of the results Scarlett found on PimEyes, including one picture that was not of her but of Britney Spears. (The blurring around the edges was done by PimEyes.)

Processing the results

It took Scarlett time to process what she was seeing in the results, which included images related to the forced sex acts that were posted on numerous websites.

At first, she thought it was her face pasted on someone else's body; then, she wondered, why did she look so young? She saw one image of her face, in which she recalls she was sitting down; she recognized the shirt she was wearing in the photo, and the hair.

She sent me this photo, which appears benign without Scarlett's context — it shows a younger version of herself, with dark brown hair parted in the center, a silvery necklace around her neck, wearing a turquoise tank top.

HAZEL TANG/CNN

She saved a copy of this image and used it to conduct another search, which she said yielded dozens more explicit images, many aggregated on various websites. Some images were posted to websites devoted to torture porn, with words like "abuse," "choke," and "torture" in the URLs.

"And it was just like," Scarlett said, pausing and making a kind of exploding-brain sound as she described what it was like to stare at the images. In an instant, she realized how memories she had of her brief time in New York didn't all match up with what was in the photos.

"It's like there's this part of my brain that's hiding something, and part of my brain that's looking at something, and this other part of my brain that knows this thing to be true, and they all just collided into each other," she said. "Like, this thing is no longer hidden from you."

Adam Massey, a partner at CA Goldberg Law who specializes in issues such as non-consensual pornography and technology-facilitated abuse, said for many people he's worked with it can feel like "a whole new violation" every time a victim encounters these sorts of images.

"It's incredibly painful for people and every time it's somewhere new it is a new jolt," he said.

Not only did Scarlett see more clearly what had happened to her, she also knew that anyone who looked her up via PimEyes could find them. Whereas in past decades such imagery might be on DVDs or photos or VHS tapes, "it's forever on the internet and now anybody can use facial-recognition software and find it," she said.

Opting out

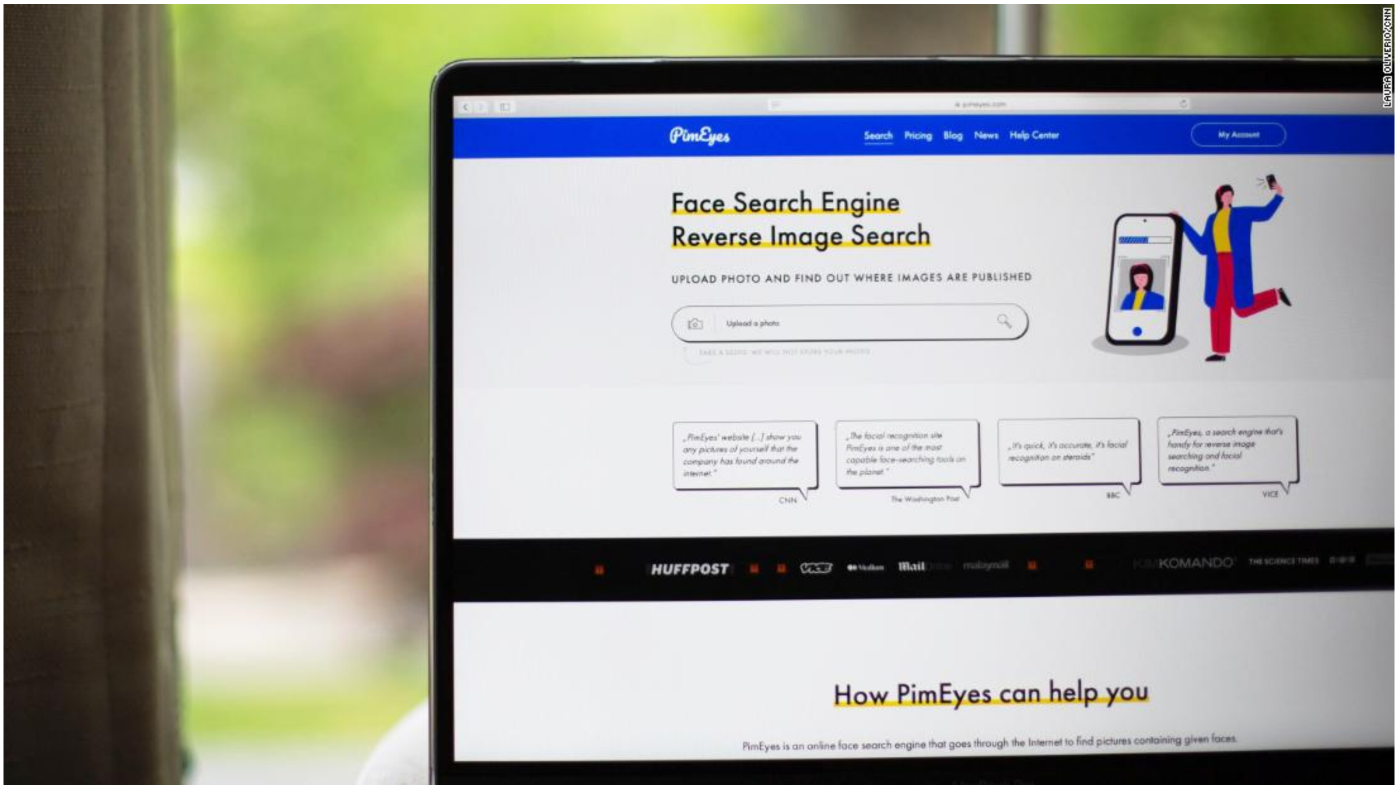
Scarlett quickly upgraded her PimEyes subscription to the $80-per-month service, which helps people "manage" their search results, such as by omitting their image results from PimEyes' public searches.

Scarlett got help in sending out DMCA takedown requests to websites hosting images she wanted taken down, she said. She isn't the copyright owner of the images, however, and the requests were ignored.

Scarlett is angry that people don't have the right to opt in to PimEyes. The website doesn't require users to prove who they are before they can search for themselves, which might prevent some forms of use or abuse of the service (say, an employer looking up prospective employees or a stalker looking up victims).

Gobronidze said PimEyes operates this way because it doesn't want to amass a large database of user information, such as photographs and personal details. It currently stores facial geometry associated with photos, but not photos, he said.

"We do not want to turn into a monster that has this huge number of people's photography," he said.


LAURA OLIVERIO/CNN
PimEyes
Search Pricing Blog News Help Center
My Account
Face Search Engine
Reverse Image Search
UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED
Upload a photo
„PimEyes' website [...] show you any pictures of yourself that the company has found around the internet."
CNN
„The facial recognition site PimEyes is one of the most capable face-searching tools on the planet."
The Washington Post
„It's quick, it's accurate, it's facial recognition on steroids"
BBC
„PimEyes, a search engine that's handy for reverse image searching and facial recognition."
VICE
HUFFPOST
VICE
Mail
KOMANDO
THE SCIENCE TIMES
How PimEyes can help you
PimEyes is an online face search engine that goes through the Internet to find pictures containing given faces.

PimEyes is a facial-recognition website meant to be used to find pictures of yourself from around the web — ostensibly to help stamp out issues such as revenge porn and identity theft.

Users can opt out of PimEyes' search results for free, but Scarlett's story shows this detail can be easy to miss. Users first have to find the link (it's in tiny gray text atop a black background on the bottom right of PimEyes' website); it requires filling out a form, uploading a clear image of the person's face, and verifying their identity with an image of an ID or passport.

"It's definitely not very accessible," said Lucie Audibert, legal officer with London-based human rights group Privacy International.

Gobronidze said the option to opt out will become easier to find with a website update that's in the works. He also shared a link that anyone can use to request PimEyes take data pertaining to specific photos of their face out of its index, which he said will become easier to find in the future as well. He also wants users to know they don't need to pay to opt out, and said the company plans to publish a blog post about the opt-out process this week.

Scarlett did opt out, saying she asked PimEyes to remove her images from its search results in mid-March.

She hadn't heard anything from PimEyes as of April 2, when she chronicled what she went through on Medium — a decision she made in part because she was hoping PimEyes would respond by honoring her request.

It was about more than that, though, she said.

"We need to look at facial recognition software and how it's being used, in terms of [how] we're losing our anonymity but also the far-reaching consequences of losing that anonymity and letting anybody put in a picture of our face and find everywhere we've been on the internet or in videos," she said.

Also in early April, Scarlett upgraded to PimEyes' $300 "advanced" tier of service, which includes the ability to conduct a deeper web search for images of your face. That yielded yet more explicit pictures of herself.

On April 5 — three days after publishing her Medium post and tweeting about her experience — PimEyes approved Scarlett's request to opt out of its service, according to an email from PimEyes that Scarlett shared with

CNN Business.

"Your potential results containing your face are removed from our system," the email said.

Gobronidze told CNN Business that PimEyes generally takes no more than 24 hours to approve a user's opt-out request.

"The images will resurface"

But as of May 19, plenty of images of Scarlett — including sexually explicit ones — were still searchable via PimEyes. I know because I paid $30 for one month's access to PimEyes and searched for images of Scarlett with her permission.

First, I tried using the recent picture of Scarlett that appears in this article — a photo she took in May. PimEyes reported 73 results, but only showed me two of them: one of Scarlett with bleached hair, which led to a dead link, and another of her smiling slightly, which led to a podcast episode in which she was interviewed.

Below the results, PimEyes's website encouraged me to pay more: "If you would like to see what results can be found using a more thorough search called Deep Search, purchase the Advanced plan," it read, with the last four words underlined and linked to PimEyes' pricing plans.

Next, I tried an image of Scarlett from 2005 that she instructed me to use: the one of her in a sleeveless turquoise top with a necklace on, which she said was the same image she sent to PimEyes to opt her out of its search results. The results were far more disturbing.

Alongside a handful of recent photos of Scarlett from news articles were numerous sexually explicit images that appeared to be from the same time period as the image I used to conduct the search.

This shows the opt-out process "sets people up to fight a losing battle," Hartzog, the law professor, said, "because this is essentially like playing whack-a-mole or Sisyphus forever rolling the boulder up the hill."

"It will never stop," he said. "The images will resurface."

Gobronidze acknowledged that PimEyes' opt-out process doesn't work how people expect. "They simply imagine that they will upload a photo and this photo will disappear from the search results," he said.

The reality is more complicated: Even after PimEyes approves an opt-out request and blocks the URLs of similar-seeming photos, it can't always stamp out all images of a person that have been indexed by the company. And it's always possible that the same or similar photos of a person will pop up again as the company continuously crawls the internet.

Gobronidze said users can include multiple pictures of themselves in an opt-out request.

Scarlett still has questions, such as what PimEyes plans to do to prevent what happened to her from happening to anyone else. Gobronidze said part of this will come via making it clearer to people how to use PimEyes, and through improving its facial-recognition software so that it can better eliminate images that users don't want to show up in the site's search results.

"We want to ensure that these results are removed for once and all," he said.

Scarlett, meanwhile, remains concerned about the potential for facial-recognition technology in the future.

"We need to take a hard stop and look at technology — especially this kind of technology — and say, 'What are we doing? Are we regulating this enough?'" she said.