

A New Tool Aims to Protect Protesters From Facial Recognition With Deepfakes

In an era in which facial recognition has made it easy for law enforcement and other organizations to search someone's identity based on their face alone, the question of when it's appropriate to share identifiable photos of protesters and activists publicly has become a flashpoint on social media.

A German startup called Brighter AI is aiming to provide a limited workaround to that problem with a new free service that draws on the same artificial intelligence tech that powers deepfakes. The tool, called #ProtectPhoto, will gauge the layout of facial features and the general appearance of subjects in a given photo, then generate lookalike synthetic faces that are untraceable by major facial recognition systems.

While the resulting photos can sometimes be garbled or disconcerting—as is the case with any generative AI—they just as often fit seamlessly into the original photo, providing a more realistic-looking alternative to simple facial blurring. Brighter AI co-founder and CEO Marian Glaeser said the clientele using the tool in its current early-access phase range from activist-bloggers who want to upload photos to a personal page, to private non-press organizations that don't want to bother with collecting permission waivers from everyone in a given photograph.

Brighter AI's core business centers on helping corporate clients such as automakers and smart-city companies anonymize visual data using the same technology. For instance, the

company can identify and replace license plates and faces in video footage. That way, a car company can train an autonomous vehicle on realistic-looking visuals while still complying with privacy regulations such as GDPR, which prohibit the collection of personally identifiable data.

But when global antiracist protests took off in the wake of the police killings of George Floyd and other Black victims earlier this year, the company began to think about how they might use this same technology to address some of the privacy issues those activists were facing.

“This created a wave within our company where my colleagues and I said, ‘We’re sitting on this technology and providing it for the automotive industry and for smart cities. But not everyone who’s on the street—like just you and me—were able to use it,’” Glaeser said. “So we thought, ‘OK, let’s spin off a project.’”

While the use of facial recognition by law enforcement and other government entities has long been controversial, high-profile incidents of bias and misidentification and recent protests have brought renewed attention to the technology. Amazon, IBM and Microsoft have all recently committed to halt the sale of facial recognition systems to police in the face of public pressure.

And while deepfakes were recently ranked by researchers as the No. 1 criminal threat posed by AI, the technology underpinning them has uses that span well beyond fake news and other nefarious uses. Big brands have been experimenting with all kinds of commercial uses for generative AI, ranging from anonymous data to creating lifelike celebrity avatars for advertisements.

<https://www.adweek.com/digital/a-new-tool-aims-to-protect-protectors-from-facial-recognition-with-deepfakes/>