Facebook will drop its facial recognition system, but why we should be skeptical

November 10 2021, by Stavros Shiaeles

Credit: RDNE Stock project from Pexels

Facebook has announced that it will stop using its facial recognition system—the artificial intelligence software which recognizes people in photos and videos and generates suggestions about who to "tag" in them.

Facial recognition systems, like Facebook's, identify people by matching faces to digital representations of faces stored on a database. Facebook has more than a billion of these representations on file but now says it will delete them.

This announcement came barely a week after Facebook's parent company rebranded itself from Facebook to Meta. The name change reflects the company's focus on the "metaverse," a vision for the internet which uses technology like virtual reality to integrate real and digital worlds.

The name change probably also had something to do with a desire to detoxify Facebook's image. In recent years, the social media giant has been embroiled in a number of controversies—perhaps most notably the Cambridge Analytica scandal.

This saw an app use Facebook's platform to harvest personal data belonging to millions of Facebook users, which was then passed to Cambridge Analytica, a now defunct British consulting firm. In 2018, the UK's data protection watchdog, the Information Commissioner's Office, fined Facebook £500,000 for its role in the scandal.

More recently we've heard former Facebook product manager Frances Haugen claim that the platform harms children, stokes division and undermines democracy in pursuit of fast growth and "astronomical profits".

We might wonder whether the facial recognition move, too, is an attempt to present a new, responsible image focused on respecting and protecting users' privacy.

Our data is like gold

Facebook is free to join and use so it relies on another valuable product to cover its expenses—people's data.

As part of my team's research, we got permission from a group of Facebook users, and had crawlers (bots that systematically browse the internet) collect their posts and pictures—or posts and pictures which featured them. Using machine learning algorithms on this data, we were able to profile their habits and predict with high accuracy things like where they would be the next day.

In a related study, we looked at Facebook wall posts and, again using machine learning, we were able to build a psychological profile of users based on their posts. That is, we could ascertain when they were sad, happy, and so on.

If I can gather data from Facebook using a relatively simple program and come up with accurate conclusions, imagine what Facebook can do with its vast amount of data—including from our face templates—and artificial intelligence.

Amid privacy concerns about the technology, in 2019, Facebook made the facial recognition feature opt-in. Last year, Facebook agreed to pay a US$650 million settlement (roughly £480 million) after a lawsuit claimed its facial recognition system violated Illinois' Biometric Information Privacy Act.

While many might construe Meta's announcement as a positive development, I see it as a convenient distraction from, or perhaps a countermeasure to, the whistleblower testimonies presenting a company that puts profits before user safety.

It's also worth pointing out that Facebook is struggling to retain young users, so they're probably looking for ways to attract this important

group to the platform.

It's not gone completely

Meta's announcement specified facial recognition technology would be limited to "a narrow set of use cases" moving forward. This could include verifying a user's identity so they can gain access to a locked account, for example.

As such, Meta is reportedly keeping DeepFace, the algorithm behind its facial recognition technology. Meta spokesperson Jason Grosse said the company hasn't ruled out using facial recognition technology in future products. Notably, Grosse has also reportedly said the commitment to stop facial recognition doesn't apply to its metaverse products.

Grosse told the publication Recode: "We believe this technology has the potential to enable positive use cases in the future that maintain privacy, control, and transparency, and it's an approach we'll continue to explore as we consider how our future computing platforms and devices can best serve people's needs […] For any potential future applications of technologies like this, we'll continue to be public about intended use, how people can have control over these systems and their personal data, and how we're living up to our responsible innovation framework."

It's important to understand that when a person engages in a virtual reality environment in the metaverse, they will generate a range of biometric data, well beyond facial scans. For example, depending on the system, it may be possible to detect and collect eye movements, body movements, blood pressure, heart rate, and details about the users' environment.

Ultimately, the artificial intelligence accompanying the metaverse will be much more sophisticated and likely bring with it a new set of data

privacy issues.

Provided by The Conversation