1. *Close read the text for understanding*
2. *Identify all claims, evidence, and reasoning/commentary used by the author.*
3. *Write a one-page reflection, connecting this article to your own experiences, reading, or observations.*

Who Owns the Right to Your Face?

by Kara Alaimo, CNN, February 12, 2020

Imagine that someone snaps a selfie of himself at a restaurant and you appear in the background. He then uploads it to Facebook. Did you know that the picture could then be used by law enforcement officials to identify you as a suspect in a crime?

The possibility was revealed in a recent investigation by the New York Times about a company called Clearview AI that has created a facial recognition app that it says has a database of three billion pictures of people from the Internet. Users of the database upload images of people to try to identify them.

Clearview AI, according to the Times' investigation, says the database was built by scraping images from websites and social media platforms, which is prohibited by the terms of service of Facebook and other social networks. The Times says the app "goes far beyond anything ever constructed by the United States government or Silicon Valley giants." Twitter, Facebook and Google have sent letters to Clearview AI demanding that it stop using images from their platforms.

Let's think about the implications of this database for a minute. When CNET, referencing the app, tweeted the question "What if a stranger could snap your picture on the sidewalk then use an app to quickly discover your name and address?" one Twitter user replied. "A lot of women would die. That's what if."

That's exactly right. Imagine, for example, an app like this in the hands of a serial rapist who could use it to track down a woman who turned him down for a date in a bar. Or think for a second about a foreign government using it to identify people leaving the CIA headquarters so it could recruit them. Or picture it being used by a government to identify protesters at a rally. Or by a defendant to identify and intimidate jurors. The many possibilities are chilling.

The CEO of Clearview AI, Hoan Ton-That, justified his database in an interview with CNN Business' Donie O'Sullivan by saying that it only uses photos that are publicly available (or have been in the past) and that it is intended to be used by law enforcement officials to solve crimes. But even law enforcement shouldn't have access to a database with such dangerous potential for misuse.

If a law enforcement agency has a legitimate and pressing need to use facial recognition to identify a suspect, it should obtain permission from a judge -- much the same way as warrants are obtained to conduct searches. Then, law enforcement agencies should be allowed to scan public places to match the images of suspects to

people in public places, as the city of London does. But they shouldn't be using a database of every publicly posted photo on the Internet.

While Clearview AI is not currently available to the general public, there is currently nothing to prevent this or another company from offering services to the public in the future. There's also the possibility that the Clearview AI database or social networks could be hacked in order to gain access to their facial recognition functions -- or they could decide to let bad actors use their facial recognition capabilities for nefarious purposes in the future.

Indeed, Kashmir Hill, the New York Times reporter who broke the story, said in a podcast that "a technology like this in public hands is the nightmare scenario" because people would no longer be anonymous in public. She said, Google and other major technology companies have long declined to build a database like this even though they have the ability to do so. The Times noted that Google's former chairman said that the reason Google never developed such a database was because it could be utilized "in a very bad way."

No one should be able to use our faces to conduct facial recognition without our express permission. We should have a human right and a legal right to control what is done with our own faces. There is certainly precedent for this. In some states, for example, it would be illegal for a company to use my picture to promote a product without my consent. So why should a company be able to profit off of using my face in other ways without my explicit permission?

In Illinois, companies have to get written permission to collect facial scans or other biometric characteristics that identify people. We need a national law that extends this protection to the rest of the country. In order to use a person's face for recognition purposes, a company should have to obtain their actual signature, so users are given an opportunity to really think through whether or not they want to allow it.

Facebook, for example, which also uses facial recognition technology, gives users the option to turn off its photo labeling service, Tag Suggestions. But a lot of people probably don't realize this or think through the implications of not doing so. And companies shouldn't be able to require that users consent to their faces being used in such ways as a condition of using their products without obtaining signatures, since studies suggest that most of us don't read lengthy privacy disclosures that are full of legalese.

The fact that the faces of many of us who use social media are now being harvested for profit flies in the face of our human rights and puts our safety in jeopardy. There shouldn't be an app for that.