A Stalker's Dream: Startup Scraped Billions of Images From Social Media for Facial Recognition AI

Science (https://www.outerplaces.com/science) **Artificial Intelligence** (https://www.outerplaces.com/tag?tag=Artificial_Intelligence)

K.S. Anthony Monday, 20 January 2020 - 11:14AM

Outer Places: adapted from public domain images

An artificial intelligence start-up that has scraped billions of images from social media websites – in likely violation of the sites' terms of service – for facial recognition use by law enforcement agencies is renewing concerns among privacy advocates who fear that the technology could eventually make stalking a complete stranger as easy as taking a picture. The company, ***Clearview AI, Inc.*** *(https://clearview.ai/)* , was the focus of an investigation by *New York Times* technology reporter Kashmir Hill, whose findings were published in a ***front page article*** *(https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html)* last weekend.

Compounding the concerns is the relative ***opacity*** *(https://www.nytimes.com/2020/01/20/technology/insider-*

According to information gleaned from the *Times* (we were unable to locate any patents for the

company's technology), Clearview's system, which has apparently been licensed by hundreds of law enforcement agencies and a "handful of companies for security purposes", is relatively straightforward. Officials – who can try the technology free for 30 days – upload a pic to Clearview's website or app. Its AI then returns matches from a database that was built by scraping over three billion images from websites and apps including Venmo, Facebook, and YouTube. In a ***FAQ*** *(https://int.nyt.com/data/documenthelper/6690-clearview-faq/c8b081a0bcca12e7903a/optimized/full.pdf#page=1)* obtained by the *Times*, the company explains:

"When you upload a photo to Clearview ,our software analyzes the hundreds of features that make up the face and search for a matching face in our image database. Whether the software finds no results, similar results, or possible results is determined by how closely the facial features match those of another face in our database . The certain that the uploaded face and search results match, the lower the delta number will be. You can find the delta number by hovering over the word 'possible' or 'similar' in the search results."

The same document claims that "Clearview has the most accurate facial identification software in the world, with a 98.6% accuracy rate" and that although the company had a 30-60% hit rate, they were "adding hundreds of millions of new faces every month and expect to get to 80% by the end of 2019."

While none of this is terribly surprising, what is troubling is that the app's programming contains code that could turn essentially arm anyone with the technology. Hill reports that "the computer code underlying its app... includes programming language to pair it with augmented-reality glasses; users would potentially be able to identify every person they saw. The tool could identify activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew."

Yashar Ali 🐘
@yashar

I've had two demos of Clearview & the results were frightening/stunning in their accuracy. Both demonstrations involved me giving blurry screenshots of a video & Clearview was able to identify both people (friends who had consented) even though they barely have a presence online twitter.com/oliviasolon/st…

> **Olivia Solon** @oliviasolon
> Bloody hell. 600 law enforcement agencies have been quietly using a face recognition app that has scraped 3bn images from YouTube,

While a ***memo*** *(https://int.nyt.com/data/documenthelper/6689-clearview-legal-memo/c8b081a0bcca12e7903a/optimized/full.pdf#page=1)* provided by Clearview to potential clients outlines the legality of the technology as it relates to law enforcement (it positions Clearview "as a search engine of publicly available images," that "pulls and compiles publicly available images from across the Internet into a proprietary image database to be used in combination with Clearview's facial recognition technology," which makes it seem more like ***Yandex*** *(https://yandex.com/)* than Black Mirror), it does not address the potential for abuse. As the Times reports, both police and Clearview's investors believe access to the technology is likely to made available to the public at some point in the future. When asked about this by Hill, Ton-That acknowledged that his invention could very well open the door to stalkers, saying that "there's always going to be a community of bad people who will misuse it."

And of course he's correct. When asked about the company's misuse of Facebook's image repository, Ton-That glibly replied that "a lot of people are doing it... Facebook knows." A Facebook spokesperson responding to the Times said that the company was reviewing Clearview's use of the site and that they would "take appropriate action if we find they are violating our rules." It is unclear, however, what that action might - or even could - be. Ton-That does claim, however, that because Clearview's technology is only capable of scraping publicly available images, people who change their social media ***settings*** *(https://www.facebook.com/settings)* to disallow indexing by Google might slip under their radar.

While these concerns may remain a minor inconvenience for Ton-That and his investors who are enjoying the lack of regulation on facial recognition technology in the United States, it's a reality that other countries are taking seriously. The ***European Commission*** *(https://www.bbc.com/news/technology-51148501)* , taking its cues from the totalitarian nightmare that China has created, is considering a three to five year ban on public use of facial recognition technology throughout the EU so that sensible legislation that respects human dignity and privacy while attending to the needs of national and global security might be formulated.

Astrophysicist Suggests Earth's Light May Attract Aliens Who Wish To 'Enslave Us, Eat Us, or Destroy Us.'

Science (https://www.outerplaces.com/science) **Artificial Intelligence** (https://www.outerplaces.com/tag?tag=Artificial_Intelligence)

Earth and its inhabitants haven't exactly kept a low profile since the introduction of electric lamps in the 19th century. Once wired, it seems there was no turning back: now entire countries are dependent on fragile power grids that provide electricity that nearly mimics actual 24/7 daylight to the extent that in some cities, we have enough light pollution to all but blot out the stars.

One scientist says that may be the least of our problems; that our high light profile may make us highly visible to extraterrestrials. This scenario, however implausible, was raised by Jacco van Loon, an astrophysicist at England's Keele University, in an essay published in ***The Conversation*** *(https://theconversation.com/aliens-could-light-and-noise-from-earth-attract-attention-from-outer-space-121073)* yesterday.

"Images of the Earth at night reveal our presence in spectacular fashion," van Loon writes. "Cities and roads outline the contours of continents, while oil platforms dot the seas and ships draw lines across the ocean. This type of light, which has replaced older, incandescent sources, is unnatural. From the orange sodium or bluish mercury lamps, to white-light emitting diodes (LEDs), the artificial origin of this "spectrum" should be easy for technologically advanced aliens to spot."

> *In the coming decades* ***Earth's space agencies may be developing*** *(http://www.esa.int/esapub/bulletin/bullet103/fridlund103.pdf) the means to detect such artificial light from planets around other stars. But we may fail, if aliens believe the smartest thing to do is to keep quiet and remain in the dark.*

It's not just our streetlights and LEDs (looking at you, Times Square) that concern van Loon. He's also a bit wary of efforts like those being made by ***SETI*** *(https://www.outerplaces.com/science/item/18429-seti-ai-alien-signals)* which involve beaming radio signals into space. Moreover, our internal communications systems might also pose a security vulnerability in terms of being detected.

"Listening, van Loon says, "is much safer. But radio communication among ourselves – which

> *Unintentionally, we may already have been observed by an amused, terrified or "interested" species, who may decide to meet us to "shake hands", or come to*

enslave us, eat us, or destroy us as a precaution. We are, after all, an aggressive species ourselves.

Perhaps we might think about dimming the lights and quieting down a bit.

Related Stories

Alexa, Where's My Privacy? Amazon Reportedly Developing Emotion-Detecting Wearables

(https://www.outerplaces.com/science/item/19351-amazon-dylan-emotional-recognition)

Company With Creepy AI That Recognizes Emotions Aims to 'Understand All Things Human'

(https://www.outerplaces.com/science/item/19329-affectiva-ai-emotional-recognition)

No Surprises Here: Algorithm Proves to Be Better Than Humans in Detecting Fake

(https://www.outerplaces.com/science/item/19302-algorithm-fake-news)

Stay up to date with our weekly recap:

email@example.com Subscribe