Businessweek - Bloomberg

@lizette_chapman More stories by Lizette Chapman

Technology

Facial recognition software still gets confused by darker skin tones.

By and

26 juin 2018 à 11:00 UTC+2 Corrected 26 juin 2018 à 17:20 UTC+2

Brian Brackeen, founder of Kairos AR Inc., in Philadelphia.

Photographer: Yael Malka for Bloomberg Businessweek

A couple of years ago, as Brian Brackeen was preparing to pitch his facial recognition software to a potential customer as a convenient, secure alternative to passwords, the software stopped working. Panicked, he tried adjusting the room's lighting, then the Wi-Fi connection, before he realized the problem was his face. Brackeen is black, but like most facial recognition developers, he'd trained his algorithms with a set of mostly white faces. He got a white, blond colleague to pose for the demo, and they closed the deal. It was a Pyrrhic victory, he says: "It was like having your own child not recognize you."

At Kairos AR Inc., his 40-person facial recognition company in Miami, Brackeen says he's improved the software by adding more black and brown faces to his image sets, but the results are still imperfect. The same problem bedevils companies including Microsoft, IBM, and Amazon and their growing range of customers for similar services. Facial recognition is being used to help India's government find missing children, and British news outlets spot celebrities at royal weddings. More controversially, it's being used in a growing number of contexts by law enforcement agencies, which are often less than forthcoming about what they're using it for and whether they're doing enough about potential pitfalls. Brackeen believes the problem of racial bias is serious enough that law enforcement shouldn't use facial recognition at all.

Microsoft, IBM, and China's Face++ misidentified darker-skinned women as often as 35 percent of the time and darker-skinned men 12 percent of the time, according to a report published by MIT researchers earlier this year. The gender difference owes to a smaller set of women's faces. Such software can see only what it's been taught to see.

In recent months, major vendors say they've diversified their training data sets to include darker-colored faces and have made strides in reducing bias. Microsoft Corp. says it plans to announce on June 26 that it will release a version of its software tool Face API that now misidentifies darker-skinned women, the group for which it's most error-prone, only 1.9 percent of the time. (The company says its error rate for other groups is zero percent.) International Business Machines Corp. says its Watson Visual Recognition, which is similarly at its weakest in identifying darker-skinned women, gets it wrong 3.5 percent of the time. Both IBM and Microsoft acknowledge their results haven't been independently verified and that real-world error rates could be different from those for their collections of stock images. The makers of Face++ didn't respond to requests for comment.

"An inaccurate system will implicate people for crimes they didn't commit"

It's Amazon.com Inc. that may have to worry most about real-world results. On June 15 a group of Amazon shareholders sent the company a letter asking it to stop marketing its Rekognition system to police departments and other government agencies until guidelines are developed to ensure the software isn't leading to civil rights violations. In another letter the following week, Amazon workers asked Chief Executive Officer Jeff Bezos to stop selling Rekognition to law enforcement agencies given "the U.S.'s increasingly inhumane treatment of refugees and immigrants." Amazon declined to comment for this story.

Government agencies have no broadly agreed-upon standards for evaluating facial recognition systems. A 2016 study by Georgetown University found that almost none of the law enforcement agencies that use facial recognition require suppliers to meet a minimum threshold for overall accuracy, let alone racial disparities. "An inaccurate system will implicate people for crimes they didn't commit and shift the burden to innocent defendants to show they are not who the system says they are," says Jennifer Lynch, senior staff attorney for the Electronic Frontier Foundation, an advocate for civil liberties online.

And the problem isn't just in the U.S. This spring, a report from Big Brother Watch, a U.K. civil rights group that examined public-records requests made to several law enforcement agencies using facial recognition, concluded that the systems were terrible. For example, the South Wales Police, which used facial recognition to screen people at public events, reported more than 90 percent of the matches were erroneous. The department said in a statement on its website that the use of facial recognition had been a "resounding success." It didn't respond to an interview request.

Makers of facial recognition technology, including Microsoft and IBM, have said the software continues to be a work in progress, with engineers focused on improving accuracy and transparency around how the improvements are being made. They say the technology has helped bust sex traffickers and apprehend would-be terrorists, though they've provided few details.

Andrew Ferguson, a law professor at the University of the District of Columbia and the author of *The Rise of Big Data Policing*, says using the powerful technology while it's still under development with scant regulation is dangerous. Law enforcement agencies have consistently botched their adoption of novel tech. "Police are beta-testing new technologies or piloting new ideas in policing without a vetting process to think through bias or how it might affect citizens' civil rights," he says.

Engineers are improving how they train algorithms as more agencies purchase the software, but they may not be able to head off growing calls for regulation. The authors of the Georgetown report call for state and federal laws governing how police departments use facial recognition and call on the police to test regularly for algorithmic bias. In April a group of civil rights organizations said it was “categorically unethical” to deploy real-time facial recognition analysis of footage captured by police body cameras.

Some, including the EFF’s Lynch, argue that their concerns will only increase as the technology improves. An accurate image merged with personal information about an individual such as location, family ties, voting records, and the like can be pulled together by authorities using products such as those from Palantir Technologies Inc. to create a digital dossier on people without their consent or knowledge. “Even if we have a 100 percent accurate system, I don’t want that system,” Lynch says. “That means we can no longer walk around and interact with people without the government knowing who we are, where we are, and who we’re talking to.”

(Corrects Microsoft error rate in fourth paragraph)

BOTTOM LINE - Microsoft says it’s cut its facial recognition error rate to zero percent for everyone except darker-skinned women, but as with rivals, those numbers are likely to rise in the real world.

July 2, 2018