The New York Times

https://nyti.ms/36SVOZE

Many Facial-Recognition Systems Are Biased, Says U.S. Study

Algorithms falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces, researchers for the National Institute of Standards and Technology found.

By **Natasha Singer** and **Cade Metz**

Dec. 19, 2019

The majority of commercial facial-recognition systems exhibit bias, according to a study from a federal agency released on Thursday, underscoring questions about a technology increasingly used by police departments and federal agencies to identify suspected criminals.

The systems falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces, the National Institute of Standards and Technology reported on Thursday. Among a database of photos used by law enforcement agencies in the United States, the highest error rates came in identifying Native Americans, the study found.

The technology also had more difficulty identifying women than men. And it falsely identified older adults up to 10 times more than middle-aged adults.

The new report comes at a time of mounting concern from lawmakers and civil rights groups over the proliferation of facial recognition. Proponents view it as an important tool for catching criminals and tracking terrorists. Tech companies market it as a convenience that can be used to help identify people in photos or in lieu of a password to unlock smartphones.

Civil liberties experts, however, warn that the technology — which can be used to track people at a distance without their knowledge — has the potential to lead to ubiquitous surveillance, chilling freedom of movement and speech. This year, San Francisco, Oakland and Berkeley in California and the Massachusetts communities Somerville and Brookline banned government use of the technology.

"One false match can lead to missed flights, lengthy interrogations, watch list placements, tense police encounters, false arrests or worse," Jay Stanley, a policy analyst at the American Civil Liberties Union, said in a statement. "Government agencies including the F.B.I., Customs and Border Protection and local law enforcement must immediately halt the deployment of this dystopian technology."

The federal report is one of the largest studies of its kind. The researchers had access to more than 18 million photos of about 8.5 million people from United States mug shots, visa applications and border-crossing databases.

The National Institute of Standards and Technology tested 189 facial-recognition algorithms from 99 developers, representing the majority of commercial developers. They included systems from Microsoft, biometric technology companies like Cognitec, and Megvii, an artificial intelligence company in China.

The agency did not test systems from Amazon, Apple, Facebook and Google because they did not submit their algorithms for the federal study.

The federal report confirms earlier studies from M.I.T. that reported that facial-recognition systems from some large tech companies had much lower accuracy rates in identifying the female and darker-skinned faces than the white male faces.

"While some biometric researchers and vendors have attempted to claim algorithmic bias is not an issue or has been overcome, this study provides a comprehensive rebuttal," Joy Buolamwini, a researcher at the M.I.T. Media Lab who led one of the facial studies, said in an email. "We must safeguard the public interest and halt the proliferation of face surveillance."

Although the use of facial recognition by law enforcement is not new, new uses are proliferating with little independent oversight or public scrutiny. China has used the technology to surveil and control ethnic minority groups like the Uighurs. This year,

United States Immigration and Customs Enforcement officials came under fire for using the technology to analyze the drivers' licenses of millions of people without their knowledge.

Biased facial recognition technology is particularly problematic in law enforcement because errors could lead to false accusations and arrests. The new federal study found that the kind of facial matching algorithms used in law enforcement had the highest error rates for African-American females.

"The consequences could be significant," said Patrick Grother, a computer scientist at N.I.S.T. who was the primary author of the new report. He said he hoped it would spur people who develop facial recognition algorithms to "look at the problems they may have and how they might fix it."

But ensuring that these systems are fair is only part of the task, said Maria De-Arteaga, a researcher at Carnegie Mellon University who specializes in algorithmic systems. As facial recognition becomes more powerful, she said, companies and governments must be careful about when, where, and how they are deployed.

"We have to think about whether we really want these technologies in our society," she said.