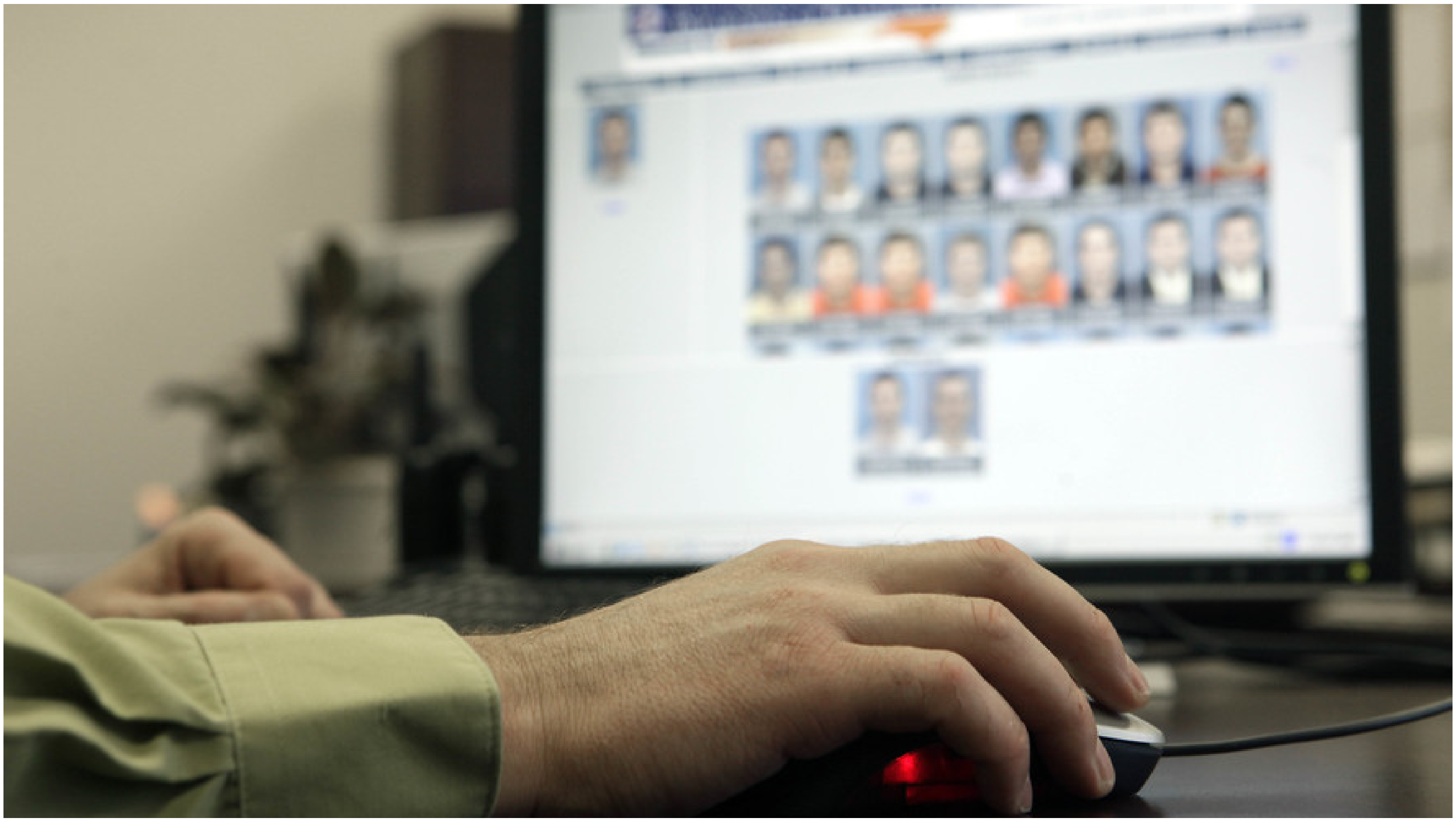
Facial-recognition technology seems to unfairly target minorities

By Sam Levin, The Guardian, adapted by Newsela staff on 10.24.16

Word Count **1,006**
Level **1240L**



Stephen Lamm, a supervisor with the ID Fraud Unit of the North Carolina Department of Motor Vehicles, looks through photos in the facial recognition system, September 24, 2009, Raleigh, North Carolina. AP Photo/Gerry Broome

According to new research, half of all American adults are included in databases that police use to identify citizens using facial-recognition technology. The news raises serious concerns about privacy violations. It also raises questions about the widespread use of racially biased surveillance technology, such as video cameras, facial-recognition software and other tools for monitoring people.

A report from Georgetown Law's Center on Privacy and Technology found that more than 117 million adults are included in a type of online "lineup." Law enforcement offices across the U.S. can scan their photos and use software to track people in these government data sets. Concerns have come up because the software is not regulated and people with no criminal history can be tracked.

Numerous police departments have face-recognition technology that allows cameras to scan people on the street, the report found. The technology tries to match these faces to the images in the police database. In Maryland, police have used software to identify faces in protest photos and match them to people with warrants, according to the American Civil Liberties Union (ACLU).

The report's findings, along with revelations from the ACLU on police monitoring in Baltimore, suggest that the technology may be violating the rights of millions of Americans, supporters said. It also said the technology could be affecting communities of color at rates that are out of proportion with their populations.

Face Recognition Challenges Our Basic Freedom

"Face recognition, when it's used most aggressively, can change the nature of public spaces," said Alvaro Bedoya, executive director of Georgetown's privacy and technology center. "It can change the basic freedom we have to go about our lives without people identifying us from afar and in secret."

The center's yearlong investigation, which was based on more than 100 police records requests, has produced the most comprehensive survey of facial databases to date. It raises numerous questions about the lack of transparency and privacy protections.

Law enforcement identity databases have traditionally captured DNA profiles related to criminal arrests or scientific investigations. What's alarming about the FBI's "face-recognition unit," according to the report, is that it is "overwhelmingly made up of noncriminal entries."

The FBI database photos come from state driver's licenses, passports and visa applications. It makes it easy for police to identify and monitor people who haven't had any run-ins with the law.

Very Few Controls Over Its Use

"In the case of face recognition, there appear to be very few controls or safeguards to ensure it's not used in situations in which people are engaged in First Amendment activity," said Neema Singh Guliani, ACLU's legislative counsel. This means people who are exercising their right to free speech could be subject to more scrutiny by the police.

For example, the ACLU recently found that police in Baltimore may have used the recognition technology along with social media accounts during high-profile police protests last year. They used the technology to identify and arrest people with outstanding warrants. That alleged surveillance relied on tools from Geofeedia, a controversial social media monitoring company that partners with police.

On Tuesday, the ACLU urged the U.S. Department of Justice to investigate facial recognition. The group also revealed last week that Facebook and Twitter had provided users' data to Geofeedia, with records suggesting that the social media sites had aided police in watching protesters. The social media sites have since cut off Geofeedia's special access to their data.

Is The Process Biased And Inaccurate?

In addition to concerns about illegal monitoring and the targeting of lawful protesters, research has found that the facial-recognition process can be biased and inaccurate. It can bring serious consequences for innocent people.

“This technology is powerful, but it is not neutral,” said Bedoya. “This technology makes mistakes.”

The FBI’s own numbers suggest that 1 out of every 7 searches of its facial-recognition database fails to turn up a correct match, the report said. This means the software occasionally produces 50 “potential” matches who are all “innocent,” it said.

Additionally, a 2012 study found that leading facial-recognition processes were up to 10 percent less accurate for African-Americans compared with white people, the ACLU noted. The study was co-authored by an FBI expert.

People Of Color Are At A Disadvantage, Some Say

What's more, the flawed computer processes can worsen biased policing practices, because they rely on mugshot databases that represent people of color at a higher rate.

For example, the Maricopa County sheriff’s office in Arizona arrests African-American residents at a rate three times higher than their share of the state population. A federal judge also found that police have racially profiled Latinos.

Those differences feed into the databases, and Arizona has no law restricting police use of facial recognition, according to the ACLU. The Maricopa sheriff’s system does not require an officer to have reasonable suspicion of a crime before searching a face in the database.

In Baltimore, some policing strategies have resulted in tens of thousands of arrests for minor offenses. Prosecutors ultimately dropped the cases.

Is Technology Being Misused?

That means many people, the vast majority of whom are people of color, may remain in facial databases even if they weren’t charged with a crime, said David Rocah. He is senior staff attorney with the ACLU of Maryland.

“A great many of those folks ... never should’ve been arrested in the first place and were innocent of any wrongdoing,” he said.

Supporters of these surveillance tools are “playing catch-up” with the technology, which has rolled out across the U.S. with little oversight or restriction, Guliani said. “That’s really a backwards way to approach it.... This is already being used against communities it’s designed to protect.”

Baltimore and Maricopa police officials did not respond to requests for comment.

Stephen Moyer is secretary of the Maryland department of public safety and correctional services, which operates the state’s facial-recognition database. He defended police use of the software. “Maryland law enforcement agencies make use of all legally available technology to aggressively pursue all criminals,” he said in a statement.