www.washingtonpost.com /business/2024/10/06/police-facial-recognition-secret-false-arrest/

Police seldom disclose use of facial recognition despite false arrests

Douglas MacMillan, David Ovalle, Aaron Schaffer ⋮ 15-20 minutes ⋮ 10/6/2024

Hundreds of Americans have been arrested after being connected to a crime by facial recognition software, a Washington Post investigation has found, but many never know it because police seldom disclose their use of the controversial technology.

Police departments in 15 states provided The Post with rarely seen records documenting their use of facial recognition in more than 1,000 criminal investigations over the past four years. According to the arrest reports in those cases and interviews with people who were arrested, authorities routinely failed to inform defendants about their use of the software — denying them the opportunity to contest the results of an emerging technology that is prone to error, especially when identifying people of color.

In fact, the records show that officers often obscured their reliance on the software in public-facing reports, saying that they identified suspects “through investigative means” or that a human source such as a witness or police officer made the initial identification.

In Evansville, Ind., for example, police said they identified a man who beat up a stranger on the street from his tattooed arms, long hair and previous jail booking photos. And in Pflugerville, Tex., police said they learned the name of a man who helped steal $12,500 in merchandise from Ulta Beauty “by utilization of investigative databases.”

Both of these suspects were identified with the aid of facial recognition, according to internal police records — information that was never shared with the accused, according to them or their attorneys. A spokeswoman for Pflugerville declined to answer questions about this case. Evansville police did not respond to requests for comment.

The Post requested records from more than 100 police departments that have publicly acknowledged using facial recognition; only 30 provided arrest records from cases in which they used the software. Most declined to answer questions about their use of the technology. A few said they use it to identify potential leads but never make an arrest based solely on a computer match, so they’re not required to disclose it to the people arrested.

The Coral Springs Police Department in South Florida instructs officers not to reveal the use of facial recognition in written reports, according to operations deputy chief Ryan Gallagher. He said investigative techniques are exempt from Florida’s public disclosure laws.

“Please do not document this investigative lead,” a department message appended to each photo search result says.

The department would disclose the source of the investigative lead if it were asked in a criminal proceeding, Gallagher added.

Defense lawyers and civil rights groups argue that people have a right to know about any

software that identifies them as part of a criminal investigation, especially a technology that has led to false arrests. The reliability of the tool has been successfully challenged in a handful of recent court cases around the country, leading some defense lawyers to posit that police and prosecutors are intentionally trying to shield the technology from court scrutiny.

Police probably “want to avoid the litigation surrounding reliability of the technology,” said Cassie Granos, an assistant public defender in Minnesota. This year, one of her colleagues helped persuade a judge to exclude a facial recognition result from the state’s case against an alleged thief because, the judge ruled, the software does not “consistently produce accurate results.”

Misidentification by this type of software played a role in the wrongful arrests of at least seven innocent Americans, six of whom were Black, according to police and court records reviewed by The Post and reports in other news outlets. Charges were later dismissed against all of them. Some were told during interrogations or in documents provided to their criminal defense lawyers that they had been identified by AI. Others learned about the software’s use only after officers mentioned in passing that “the computer” had found them, or that they had been a “positive match.”

Among them was Quran Reid, who spent six days in jail in 2022 for allegedly using stolen credit cards to buy luxury purses in Louisiana — a state he said he had never visited. A detective with the Jefferson Parish Sheriff’s Office wrote in a sworn affidavit that he had been “advised by a credible source” to look at Reid, then 28 and living in Atlanta. In fact, Reid was identified by facial recognition software that was fed a crime scene photo.

The affidavit said nothing about use of the technology; Reid learned about it from his lawyer days into his incarceration.

“Why me? Why did you pick me out of everybody?” Reid recalled thinking when he was arrested. “You don’t even know where it’s coming from,” he said in an interview with The Post.

The case was dismissed after his lawyer pointed out that Reid has a facial mole that was not present in the image of the perpetrator. Reid has since sued the sheriff and the detective. The sheriff’s department did not respond to requests for comment and it’s unclear whether the robbery for which Reid was arrested has been solved.

Facial recognition software works by submitting an image from a crime scene, often captured by video surveillance camera, to a database of photos, often from mug shots and driver’s licenses. The software uses artificial intelligence to compare the face of the person in the “probe image” to the faces in the database. It then returns photos of people it has identified who are similar in appearance. Because there is no scientific consensus on what constitutes a match, software makers vary widely in how many results they show and how closely each result resembles the probe photo.

Clearview AI, a popular maker of facial recognition software for police, compares probe images to its database of billions of images scraped from social media and public websites — which means that anybody with a photo anywhere on the web could be pulled into any criminal investigation if they happen to resemble the culprit. Clearview search results produced as evidence in one Cuyahoga County, Ohio, assault case included a photo of basketball legend Michael Jordan and a cartoon of a Black man.

In an emailed statement, Jack Mulcaire, Clearview's chief legal officer, noted that the software's first two results in that search were of the perpetrator, who later pleaded guilty. The company declined to answer other questions about its technology.

Federal testing of top facial recognition software has found the programs are more likely to misidentify people of color, women and the elderly because their faces tend to appear less frequently in data used to train the algorithms, according to Patrick Grother, who oversees biometric testing at the Washington-based National Institute of Standards and Technology. Roughly 2 million people of color and 2 million women are arrested in the United States each year, according to federal data.

Clearview's contracts with several police departments, obtained by The Post, say the program is not designed "as a single-source system for establishing the identity of an individual" and that "search results produced by the Clearview app are not intended nor permitted to be used as admissible evidence in a court of law or any court filing."

Prosecutors are required to inform defendants about any information that would help prove their innocence, reduce their sentence or hurt the credibility of a witness testifying against them. When prosecutors fail to disclose such information — known as a "Brady violation" after the 1963 Supreme Court ruling that mandates it — the court can declare a mistrial, overturn a conviction or even sanction the prosecutor.

No federal laws regulate facial recognition and courts do not agree whether AI identifications are subject to Brady rules. Some states and cities have begun mandating greater transparency around the technology, but even in these locations, the technology is either not being used that often or it's not being disclosed, according to interviews and public records requests.

In June 2023, a three-judge appeals panel in New Jersey ruled that a defendant had a right to information regarding facial recognition technology's use, saying the software's "veracity has not been tested or found reliable on an evidential basis by any New Jersey court."

The technology had been used to help identify Francisco Arteaga as the perpetrator of a 2019 armed robbery in West New York, N.J.

A lower court had turned down Arteaga's lawyer's demands for information about the technology, including the algorithm's error rate, the complete list of possible matches and the qualifications of the person who picked him as the most likely match.

The ruling set precedent in that state but other states aren't required to abide by it.

Briefed on The Post's findings, Sen. Cory Booker (D-N.J.) said that "use of AI by law enforcement that leads to criminal charges should be disclosed to safeguard constitutional rights and ensure a fair trial." Booker says he would like to see legislation passed to require disclosure, noting that "people's freedom literally hangs in the balance."

In Miami, police have kept detailed data since 2020 about the results of facial recognition searches but have rarely shared that information with defendants, according to The Post's analysis of internal software logs and corresponding court records.

Over the past four years, the Miami Police Department ran 2,500 facial recognition searches in investigations that led to at least 186 arrests and more than 50 convictions. Among the

arrestees, just 1 in 16 were told about the technology's use — less than 7 percent — according to a review by The Post of public reports and interviews with some arrestees and their lawyers. The police department said that in some of those cases the technology was used for purposes other than identification, such as finding a suspect's social media feeds, but did not indicate in how many of the cases that happened.

Carlos J. Martinez, the county's chief public defender, said he had no idea how many of his Miami clients were identified with facial recognition until The Post presented him with a list.

"One of the basic tenets of our justice system is due process, is knowing what evidence there is against you and being able to challenge the evidence that's against you," Martinez said. "When that's kept from you, that is an all-powerful government that can trample all over us."

After reviewing The Post's findings, Miami police and local prosecutors announced plans to revise their policies to require clearer disclosure in every case involving facial recognition.

In January, Miami Assistant Police Chief Armando Aguilar told a congressional panel on AI in law enforcement that his department is "the first to be completely transparent about" the use of facial recognition. But in July, after reviewing The Post's findings, Aguilar acknowledged that officers may not have always informed local prosecutors about the use of facial recognition. Aguilar said the department would give prosecutors all information on the use of facial recognition, in past and future cases, but leave it up to prosecutors to decide what to disclose to defendants. He said the department would also begin training officers to always disclose the use of facial recognition in incident reports.

> Miami Assistant Chief of Police Armando Aguilar spoke in front of a Senate subcommittee to discuss how facial recognition AI is used by his department. (Video: U.S. Senate)

Katherine Fernandez Rundle, the state attorney for Miami Dade County, said in an interview that, before being contacted by The Post, Miami police had not informed her office about their use of facial recognition in the vast majority of cases. Her office recently instructed all local police departments to include information about facial recognition in public reports and said prosecutors would be proactive in asking police whether identifications were made with AI, Ed Griffith, a spokesman for the prosecutor, said.

Rundle acknowledged that studies have raised concerns about the technology's accuracy and fairness. "You cannot rely on this for probable cause alone," she said.

However, her office said it could not commit to reviewing all 186 cases identified by The Post. In an email, Chief Assistant State Attorney Kathleen Hoague said "it is more important for us to work on a policy moving forward."

Gordon Weekes, the public defender in Broward County, just north of Miami, said his attorneys rarely encounter cases in which facial recognition is disclosed, though numerous local police agencies have access to such programs.

"How can there be any checks or balances?" Weekes said. "If law enforcement is going to embrace new technology, there's going to have to be safeguards in place so it doesn't go off the rails and start to be abusive."

Most of the police departments that provided records to The Post did not respond to or declined to answer questions about why they don't inform people about the use of facial recognition. Five defended the practice of not disclosing AI identifications.

"Our detectives utilize many tools, databases, and techniques during the course of an investigation, in which Clearview is one of them," Jessica Taylor, a spokeswoman for the city of Pflugerville, said in an email. "It is not protocol to list each of those tools, databases, or techniques in a report."

Police in Arvada, Colo., provided documents showing they have disclosed every instance of facial recognition usage since the state passed a law requiring it in 2022.

At least 21 cities and counties and the state of Vermont prohibit the use of facial recognition tools by law enforcement due to concerns about their accuracy and potential for racial bias. However, in at least two of these places, Austin and San Francisco, officers have covertly enlisted the help of neighboring law enforcement agencies that aren't subject to the same rules, The Post reported earlier this year.

In response to The Post's reporting, Austin recently rewrote its policy to outlaw that practice.

Defendants arrested after a facial recognition match said they deserve the chance to face their accuser — even when it's AI.

Despite a New Jersey appeals court ruling that Arteaga had a right to information about his AI match, the NYPD, which conducted the search for police in New Jersey, declined to provide it. Prosecutors in New Jersey reduced the charges against Arteaga as a result.

By then, Arteaga had spent four years in jail awaiting trial. Though he maintains his innocence, he said he pleaded guilty to second-degree robbery to get back to his two children. Caitlin Mota, a spokeswoman for the Hudson County prosecutor, declined to comment.

In an interview, Arteaga said he has "no problem with" police using tools like facial recognition but said they should disclose it and share how the software works.

"When you're dealing with a software whose source code is not accessible," he said, "then how is that fair?"

About this story

The Washington Post spent six months requesting internal records about facial recognition from more than 100 police departments around the country that had publicly indicated using the technology for suspect identification. More than 40 provided data about their use of the software, with 30 providing related incident reports and arrest warrants corresponding to more than 1,000 cases in the past four years.

The Post then searched court records to determine whether public documents disclosed use of the technology. The Post also contacted the defendants or their lawyers where contact information was available to determine whether they had been made aware of the technology's use. The vast majority said they had no idea facial recognition had been used to identify them. Not everyone could be contacted, so it's possible some additional

defendants had been told about facial recognition despite it not appearing in public documents.

The Post found that police do not always clearly label their use of the software. For example, in data provided by the Miami Police Department, records show that the victims knew the suspects in some cases where facial recognition was listed as leading to a “Positive ID.” The department said officers sometimes use facial recognition tools to locate a known suspect’s social media profile and other digital information.

Editing by Evelyn Larrubia. Jeremy Merrill and Nate Jones contributed to this report.