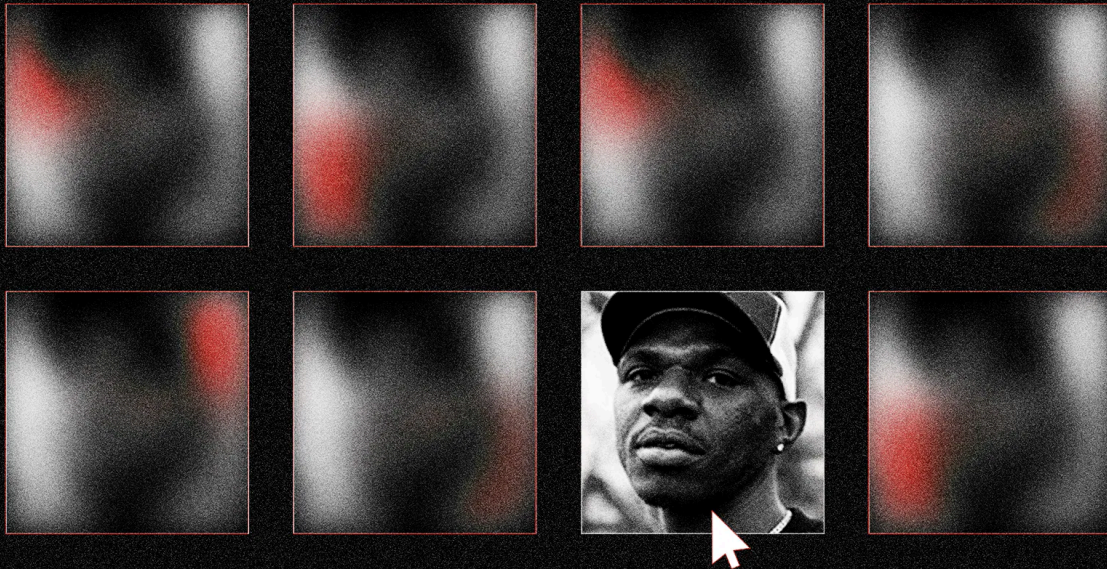


EXCLUSIVE

Arrested by AI: Police ignore standards after facial recognition matches

Confident in unproven facial recognition technology, sometimes investigators skip steps; at least eight Americans have been wrongfully arrested.



(Illustration by Lucy Naland/The Washington Post; Kaiti Sullivan for The Washington Post)

By [Douglas MacMillan](#), [David Ovalle](#) and [Aaron Schaffer](#)

Today at 1:30 p.m. EST

24 min 455

PAGEDALE, Missouri — After two men brutally assaulted a security guard on a desolate train platform on the outskirts of St. Louis, county transit police

detective Matthew Shute struggled to identify the culprits. He studied grainy surveillance videos, canvassed homeless shelters and repeatedly called the victim of the attack, who said he remembered almost nothing because of a brain injury from the beating.

Months later, they tried one more option.

Shute uploaded a still image from the blurry video of the incident to a facial recognition program, which uses artificial intelligence to scour the mug shots of hundreds of thousands of people arrested in the St. Louis area. Despite the poor quality of the image, the software spat out the names and photos of several people deemed to resemble one of the attackers, whose face was hooded by a winter coat and partially obscured by a surgical mask.

Though the city's facial recognition policy warns officers that the results of the technology are "nonscientific" and "should not be used as the sole basis for any decision," Shute proceeded to build a case against one of the AI-generated results: Christopher Gatlin, a 29-year-old father of four who had no apparent ties to the crime scene nor a history of violent offenses, as Shute would later acknowledge.

Arrested and jailed for a crime he says he didn't commit, it would take Gatlin more than two years to clear his name.

A Washington Post investigation into police use of facial recognition software found that law enforcement agencies across the nation are using the artificial intelligence tools in a way they were never intended to be used: as a shortcut to finding and arresting suspects without other evidence.

Most police departments are not required to report that they use facial recognition, and few keep records of their use of the technology. The Post reviewed documents from 23 police departments where detailed records about facial recognition use are available and found that 15 departments spanning 12 states arrested suspects identified through AI matches without any independent evidence connecting them to the crime — in most cases contradicting their own internal policies requiring officers to corroborate all leads found through AI.

Some law enforcement officers using the technology appeared to abandon traditional policing standards and treat software suggestions as facts, The Post found. One police report referred to an uncorroborated AI result as a "100%

match.” Another said police used the software to “immediately and unquestionably” identify a suspected thief.

Gatlin is one of at least eight people wrongfully arrested in the United States after being identified through facial recognition. Six cases were previously reported in media outlets. Two wrongful arrests — Gatlin and Jason Vernau, a Miami resident — have not been previously reported.

All of the cases were eventually dismissed. Police probably could have eliminated most of the people as suspects before their arrest through basic police work, such as checking alibis, comparing tattoos, or, in one case, following DNA and fingerprint evidence left at the scene.

What went wrong

In eight known cases of wrongful arrests involving facial recognition, police failed to take one or more basic investigative steps.

In 6 cases:

Police failed to check alibis

Quran Reid was arrested for allegedly stealing purses from a Louisiana store even though he repeatedly told the officers who arrested him in his hometown of Atlanta that he’d never been to the state. Investigators never sought proof he was at work in Georgia on the day the crime was committed.



(John Bazemore/AP)

In 2 cases:

Police ignored evidence that contradicted their theory

Police in Woodbridge, New Jersey, were so intent on building a case against Nijeer Parks, a robbery suspect, that they cast aside DNA and fingerprint evidence pointing to another potential suspect.

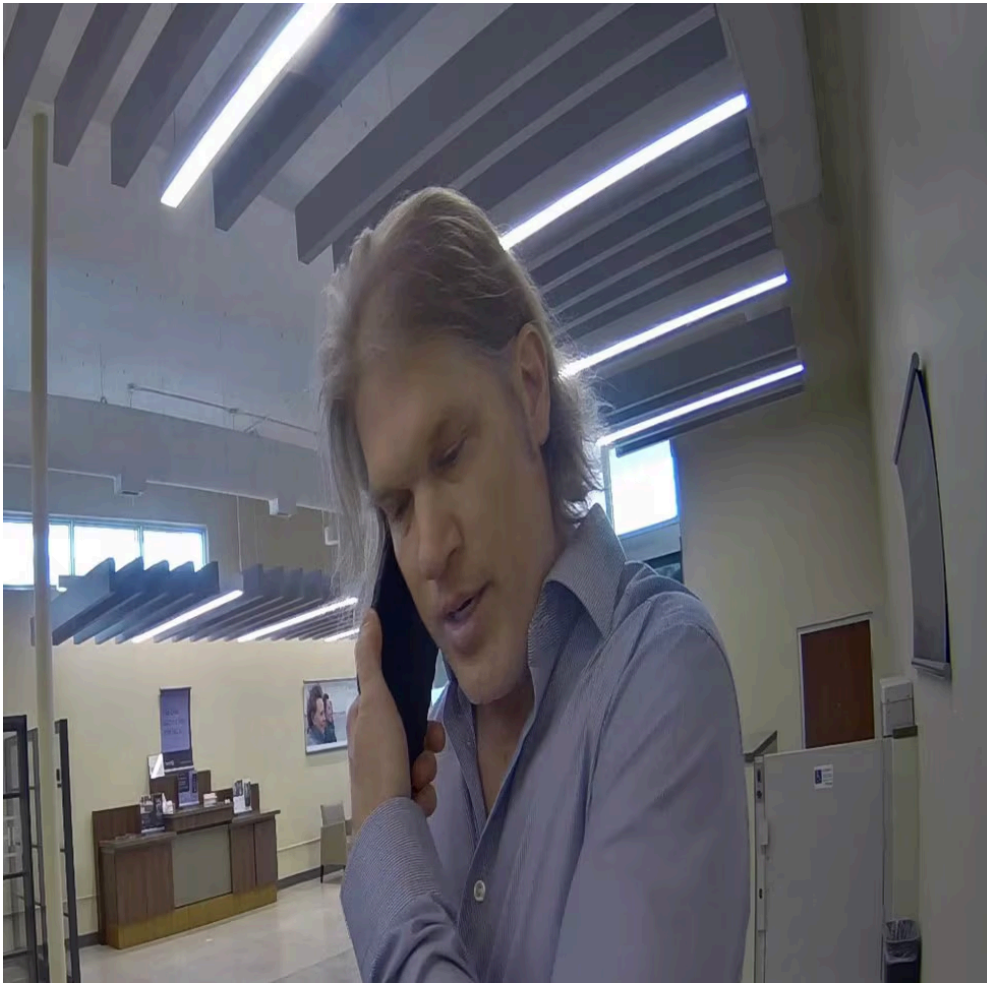
SIGNATURE OF PERSON FINGERPRINTED		SOCIAL SECURITY NO.		LEAVE BLANK						
ALIASES/MAIDEN LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX										
FBI NO. 362204AE1	STATE IDENTIFICATION NO.	DATE OF BIRTH MM DD YY	SEX	RACE	HEIGHT	WEIGHT	EYES	HAIR		
1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. PINKY						
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. PINKY						
FINGERPRINTS TAKEN SIMULTANEOUSLY		L. THUMB	R. THUMB	C746DN_Holmde 12-14 06:08:46						
		FINGERPRINTS TAKEN SIMULTANEOUSLY								

(Court Records)

In 5 cases:

Police failed to collect key pieces of evidence

Jason Vernau spent three days behind bars after he was accused of cashing a fraudulent \$36,000 check at a Miami bank. Police had relied on an image of the wrong person and failed to check Vernau's bank accounts, his defense lawyer said.



(Office of the State Attorney)

In 3 cases:

Police ignored suspects' physical characteristics

Porcha Woodruff was seven months pregnant at the time of the carjacking Detroit police accused her of committing. She was arrested even though nothing in the surveillance images or eyewitness statements indicated the involvement of a pregnant woman.



(Court Records)

In 6 cases:

Police relied on problematic witness statements

After Detroit police used facial recognition to identify Robert Williams as a suspect in a watch theft at a high-end store, his identity was confirmed by a security person who was not present for the crime.



Q: Do You see anyone you recognize?

A: Yes

Q: If the answer to question #1 was yes, identify by number the photo(s) you recognize.

A: #3

(Court Records)

These examples of questionable police work — gleaned through The Post’s analysis of rarely seen internal software records, arrest reports, court records, and interviews with police, prosecutors and defense lawyers — are probably a small sample of the problem. The total number of false arrests fueled by AI matches is impossible to know, because police and prosecutors rarely tell the public when they have used these tools and, in all but seven states, no laws explicitly require it to be disclosed.

Hundreds of police departments in Michigan and Florida have the ability to run images through statewide facial recognition programs, but the number that do so is unknown. One leading maker of facial recognition software, Clearview AI, has said in a pitch to potential investors that 3,100 police departments use its tools — more than one-sixth of all U.S. law enforcement agencies. The company does not publicly identify most of its customers.

Through a review of government contracts, media reports, and public records requests, The Post identified 75 departments that use facial recognition, 40 of

which shared records on cases in which it led to arrests. Of those, 17 failed to provide enough detail to discern whether officers made an attempt to corroborate AI matches. Among the remaining 23 agencies, The Post found that nearly two-thirds had arrested suspects identified through AI matches without independent evidence.

Most of the departments declined to answer questions about their use of AI. Some denied that officers arrested people based on AI alone, but declined to provide details or documents to support these claims.

Others said that officers can determine if the person they see in two or more photos is the same. In Florence, Kentucky, documents show, police arrested people identified by facial recognition without independent corroboration in four cases. One pleaded guilty to theft; the other three cases are still pending.

The local prosecutor, Louis Kelly, said he trusts officers to use their judgment in identifying suspects, including those found with AI.

“We have to allow officers to use common sense and available methods,” Kelly said in an email.



Christopher Gatlin was arrested and jailed for a crime he says he didn't commit, and it would take more than two years to clear his name. (Kaiti Sullivan for The Washington Post)

A new sense of urgency

On Aug. 9, 2021, eight months after the Pagedale train station assault, three uniformed officers appeared in the lobby of the apartment building of the injured security guard, Michael Feldman, with a new sense of urgency about solving the case.

The officers brought along a photo lineup with images of six men, including Gatlin. Feldman told them he still remembered very little about it because of the brain injury he suffered.

“It felt like I was being cornered in this situation I didn’t want to be in,” Feldman, 62, said in a recent interview. “I felt like I didn’t remember what he looked like.”

08/09/21 10:38:28 CST





Following the officer's instructions, Feldman nonetheless examined each photo and then, one by one, discarded them into a pile, according to body-camera footage included in a court filing.

Feldman narrowed the group of photos down to two — Gatlin and another man, who was also Black but had a notably lighter complexion, according to a motion filed by Gatlin's lawyer. He placed Gatlin's photo into the discard pile while motioning to the other man. "I want to say it's him," he said, pointing to the other man. The detectives did not immediately accept the identification and a few moments later, Feldman brought Gatlin's photo back, saying he wasn't sure which of them it could have been.

"Think about the characteristics of the guy, his complexion; did he have anything about his hair, or the clothing he was wearing?" St. Louis city police detective Matthew Welle asked. When Feldman said he thought the man might have been wearing a hat or stocking cap, Welle encouraged him to put his hands on the photos to help him "picture these two guys wearing a stocking cap."

Feldman then picked Gatlin and looked over at the officer expectantly.

"Okay!" Welle said, directing Feldman to circle Gatlin's photo and sign his name, ignoring his earlier comment about the other man.

Feldman's statement was the only evidence police had when they filed a complaint against Gatlin six days later, showing how police confidence in software results can influence an entire investigation. Asked months later in court whether steering the witness in this way had been proper, the lead detective, Shute, would answer "no."

Tracy Panus, a spokeswoman for the St. Louis County police, said in an emailed statement that the agency trains officers to develop "independent, corroborative evidence regarding facial recognition" and requires supervisor review of cases in which facial recognition helps lead to an arrest.

Panus, Shute and Mitch McCoy, a spokesman for the St. Louis Metropolitan Police, all declined to discuss the investigation into the attack on Feldman. Welle did not respond to requests for comment.

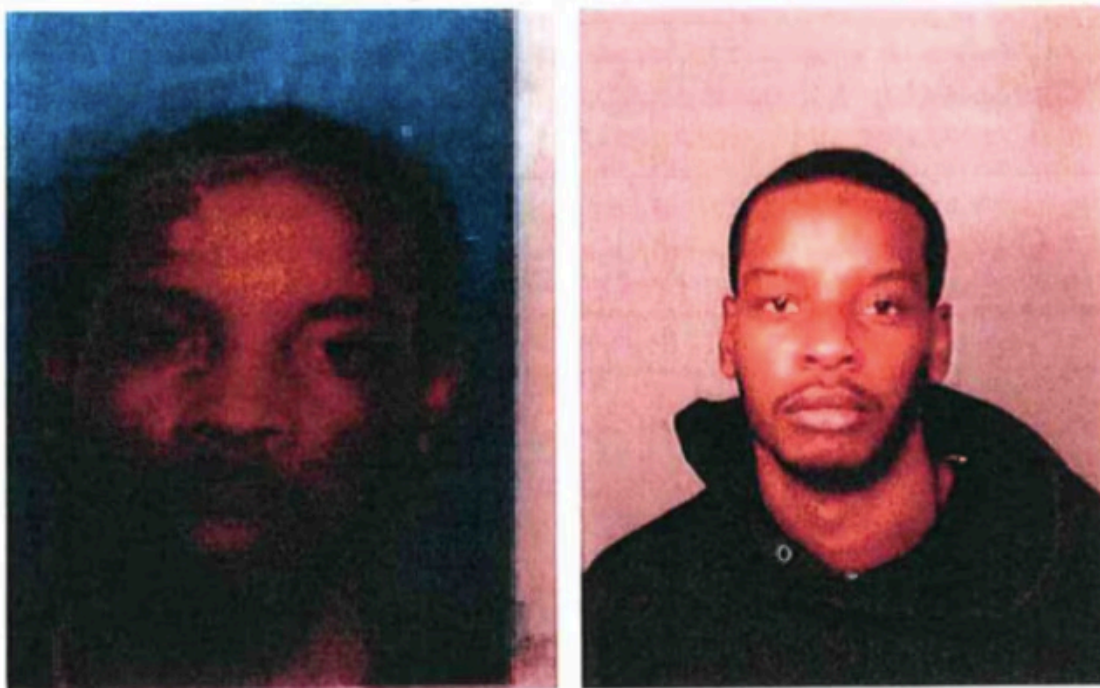
Automation bias

Police credit facial recognition with helping them solve many difficult cases, including the Jan. 6, 2021, attack on the U.S. Capitol. Federal investigators gathered copious additional evidence in that probe — including cellular location data and social media posts — resulting in more than 1,200 convictions.

The software performs nearly perfectly in lab tests using clear comparison photos. But there has been no real-world, independent testing of the technology's accuracy in how police typically use it — with lower-quality surveillance images and officers picking one candidate from a list of possible matches, said Katie Kinsey, chief of staff for the Policing Project at NYU School of Law. Because of this, it's hard to know how often the software gets it wrong, she said.

Moreover, researchers have found that people using AI tools can succumb to “automation bias,” a tendency to blindly trust decisions made by powerful software, ignorant to its risks and limitations. One 2012 [study](#) by a University College London neuroscientist found fingerprint examiners were influenced by the order in which a computer system showed them a list of potentially matching fingerprints. They were more likely to erroneously match prints that appeared at the top of the list, suggesting they failed to properly evaluate the similarities of other potential matches because of confidence in the system.

In one example of the potent power of facial recognition, police in Woodbridge, New Jersey, arrested Nijeer Parks, a robbery suspect they found through facial recognition in 2019, even though DNA and fingerprint evidence collected at the scene clearly pointed to another potential suspect, according to documents produced in a lawsuit Parks later filed against the police department. Woodbridge settled the suit for \$300,000 last year, without admitting wrongdoing. Woodbridge police did not respond to requests for comment, and The Post could find no indication that the man who was a match for the DNA and fingerprint evidence was ever charged.



Police in Woodbridge, New Jersey, had the blurry photo from a robbery suspect's driver's license, left, scanned through facial recognition software and later arrested Nijeer Parks, right, the man whose mug shot the software identified as a potential match. (Court records)

Academic research has shown some people have genetically similar doppelgängers who are unrelated to them. People are not particularly good at distinguishing between two unfamiliar faces that look alike, making it difficult to discern whether an AI match is the perpetrator, or just someone who looks like them, according to Clare Garvie, an AI researcher who has trained criminal defense lawyers around the country on how police are using facial recognition.

During a court deposition in 2023, Jennifer Coulson, a trained image examiner for the state of Michigan, described in odd detail how she determined features of a man's face matched those of the perpetrator caught on surveillance video stealing watches from a high-end store.

"I loved his facial hair growth pattern, the thickness of his lips, the fissure of his lips," said Coulson, who picked the man out of hundreds of photos returned by the state's facial recognition software as possible matches. "I loved the thickness of his cheeks ... and the presence of the sclera of the eyes."

Coulson was wrong. The face she was describing belonged to Robert Williams, whom Detroit police wrongfully arrested partly based on her finding. In a settlement announced in June, Detroit paid Williams \$300,000 and agreed to require officers to collect independent evidence on AI-identified suspects before seeking an arrest warrant. Coulson did not respond to a request for comment. A spokeswoman for the Michigan State Police declined to comment on the error,

but said the state relies on investigators to corroborate all of the leads it provides them from facial recognition.



Robert Williams of Farmington Hills, Michigan, was arrested after Detroit police using facial recognition technology mistakenly identified him as a suspected shoplifter. (American Civil Liberties Union)

In several cases reviewed by The Post, officers arrested a person identified by AI after only using their own judgment that it was the same person or by showing a photo of the suspect to witnesses, without otherwise linking the person to the crime, records show.

Long before AI, witness identification has been seen as problematic when it is the only evidence of a suspect's guilt. Human memory is imperfect, and witnesses can be unconsciously or consciously influenced by police. According to a database maintained by the National Registry of Exonerations, an academic research group, more than a quarter of all exonerations since 1989 — or 986 cases — have involved a mistaken witness identification.

Whether they realize it, police who put a suspect found through AI into a photo lineup may effectively “trick” a witness into picking that person, said Gary Wells, a psychologist at Iowa State University whose research has shed light on faulty eyewitness identifications.

The AI may have selected someone who looks so much like the perpetrator it would be impossible for many people to tell the difference, Wells said. “Of

course they're going to pick him.”

A knock at the door

Five days after Feldman circled Gatlin's photo, police knocked on the door of Gatlin's sister's house in St. Louis.

A slender man with a broad smile, Gatlin had been splitting his time between St. Louis, where he grew up, and a small town in Indiana where his dad lived. He had recently returned to St. Louis for his mother's funeral but ended up staying a while, spending time with his children and taking a job at the Walmart near the St. Louis airport.

He was unwinding after working the night shift when the two officers asked him to step outside. He complied, thinking they were there to ask about his truck, which had broken down on the side of the road.

They asked whether he had a card for the metro train in his wallet. When he said no, they briefly looked at each other, he said. Then one pulled out a pair of handcuffs and told him he was going to jail.

Like many facial recognition cases reviewed by The Post, the police complaint said only that Gatlin “has been identified” in an assault that was caught on video, without saying how police had connected him to the crime. When Gatlin could not pay the \$75,000 cash bond, he was remanded to a jail cell smaller than a parking space.

“I never thought I was going to get out,” Gatlin, now 32, said in an interview. He ended up spending 16 months in jail, in part because he cut off the ankle monitor when he was on conditional release and had to go back.

In all the known cases of wrongful arrest because of facial recognition, police arrested someone without independently connecting the person to the crime. Take Vernau, 49, a medical entrepreneur, who spent three days behind bars in July 2024 after police accused him of cashing a fraudulent \$36,000 check at a Truist bank branch in Miami, based on a surveillance camera image they ran through facial recognition, according to documents prosecutors shared with The Post.

Unlike other false arrest cases, Vernau was correctly identified as the person in the surveillance video. However, Vernau was just a customer cashing a legitimate \$1,500 check in the same bank on the same day as the fraud. An investigator from Truist mistakenly shared the clip of Vernau with police, according to a summary of the case written by a prosecutor.

The police never checked Vernau's bank accounts, the time-stamp of the transaction, or other evidence that would have revealed the mistake, his defense lawyer said.

"This is your investigative work?" Vernau recalls asking the detectives who questioned him at the Miami Police Department during his detention. "You have a picture of me at a bank and that's your proof? I said, where's my fingerprints on the check? Where's my signature?"



Jason Vernau was wrongfully jailed on suspicion of check fraud by the Miami Police Department after identifying him using facial recognition. (Scott McIntyre for The Washington Post)

Prosecutors later dropped the case, but Vernau said he is still working to get the charges removed from his record.

Freddie Cruz, a Miami police spokesman, said the department had launched an internal investigation into the handling of the case.

Truist spokeswoman Carly DeBeikes said the company is “unable to discuss any open or closed law enforcement matters.”

Vernau is White. The other seven wrongful arrestees are Black — concerning evidence of the technology’s racial bias, according to civil liberties groups. Federal testing in 2019 showed that Asian and Black people were up to 100 times as likely to be misidentified by some software as White men, potentially because the photos used to train some of the algorithms were initially skewed toward White men.

In interviews with The Post, all eight people known to have been wrongly arrested said the experience had left permanent scars: lost jobs, damaged relationships, missed payments on car and home loans. Some said they had to send their children to counseling to work through the trauma of watching their mother or father get arrested on the front lawn.

Most said they also developed a fear of police.

“I knew I was innocent, so how do I beat a machine?” said Alonzo Sawyer, 58, who was arrested by Maryland authorities in 2022 for an assault on a bus driver that occurred while he said he was at his sister-in-law’s house.

Sawyer says he only got out of jail because his wife drove 90 miles to personally confront a probation officer whom police had pressured into falsely confirming her husband as the attacker. He apologized and retracted his statement. Scott Shellenberger, the state’s attorney for Baltimore County, said in an interview that Sawyer was “wronged” and should never have been arrested.

A lucky break

Gatlin’s lucky break came in the form of his assigned public defender, Brooke Lima, whose decades of experience in criminal defense had made her wary of trusting police. The county’s case against Gatlin made no sense to her, because he had no reason to be on the train that morning.

Gatlin owned a truck and rarely took public transit. He says he thinks he was at home with his family that day, but he can’t be sure, and has nothing to prove it

because police did not approach him until eight months after the crime.

St. Louis uses a facial recognition system maintained by a regional, multi-jurisdiction law enforcement program that contains more than 250,000 mug shots. Gatlin was in the system, having been arrested for traffic violations as well as a burglary charge in 2018; the burglary charge was later dropped because prosecutors could not produce enough evidence, records show. Gatlin declined to comment on the charge, and Missouri courts do not provide records on cases that have been dismissed.

“It seemed so outrageously dystopian to me,” Lima said in an interview. “You’ve got a search engine that is determined to give you a result, and it’s only going to search for people who have been arrested for something, and it’s going to try to find somebody among that limited population that comes closest to this snippet of a half-face that you found.”

Lima had never heard of police using facial recognition before seeing it mentioned in Gatlin’s police report. She researched how it worked, spoke to a national expert on the technology and went down a “Westlaw rabbit hole,” researching the handful of appellate cases around the country in which the technology has begun to be mentioned. She became disturbed by the idea that “the government would rely on a machine to identify somebody as a potential suspect in a crime.”



St. Louis police ran this surveillance image through a facial recognition program as they sought to find one of the perpetrators of a December 2020 assault. (Court records)

Examining the surveillance videos of the train platform attackers — which were filmed by a small camera affixed to the side of a Metro bus parked at the station that morning — Lima came to believe, and eventually argued in court, that Shute

and Welle had relied on an image that was probably not clear enough to produce a reliable match.

The user manual for the St. Louis Mugshot Recognition Technology program states that an image “needs to be high quality in order for the system to provide accurate likely candidates,” and yet the detectives had submitted a photo of a man whose face was barely recognizable.

The body-cam video showing Feldman’s photo lineup did not come to light until months after Gatlin’s arrest, when an officer mentioned during a deposition that he recorded the episode. Chris King, a spokesman for the St. Louis County prosecutor, said the attorney assigned to this case first learned about the existence of the video from this deposition — even though the recording was explicitly mentioned in a police report that was provided to prosecutors and defense attorneys following the arrest.

After the prosecutor learned about the video and requested it from police, King said, it was released to the defense. St. Louis Circuit Court Judge Brian May, who presided over the case, watched it during a February 2024 hearing and immediately ruled the identification could not be used in court.

Welle and Shute had broken with widely accepted practices for conducting fair and impartial photo lineups, May found. They had pushed Feldman for a statement even though he said he couldn’t remember the perpetrators. They invited a third officer to be an impartial administrator, per protocol, but Welle interfered with the process by suggesting which photo belonged to their suspect, the judge determined.

“I really do think the detective was sort of ... over zealous to be able to try to resolve this crime,” May said, according to a court transcript.

During the hearing, Lima confronted Shute with the steps he had taken to arrest Gatlin: the surveillance image, the facial recognition scan, the improper photo lineup and witness statement.

“Do you believe that this is a reliable way to get a legitimate identification of a suspect?” she asked.

“I do not,” Shute said.

With no evidence against him, prosecutors dropped all charges against Gatlin in March. This week, he sued the agencies and officers responsible for his arrest,

seeking unspecified monetary damages. The agencies and officers did not immediately respond to a request for comment.

Meanwhile, Lima — freshly educated on police use of facial recognition technology — remains concerned that police overconfidence and lax oversight will lead to more wrongful arrests.

“What are police departments being told about how they can and should use this?” she said. “And who’s enforcing that?”

Methodology

The Post spent eight months requesting internal records about facial recognition from more than 100 police departments around the country believed to be using the technology, based on government contracts, media reports and previous public records requests. Of these, 75 confirmed their use of the software, with 40 providing records of individual cases in which they used the software. Some of the agencies said they did not keep logs of the cases in which the software was used. Others said such logs were not public information. Only 23 provided incident reports and arrest warrants that included sufficiently detailed narratives to determine how police conducted their investigations.

From these reports, The Post identified cases in which police did not appear to seek other evidence establishing an AI-selected suspect’s connection to the crime. If police made an arrest only after showing a photo of a suspect identified by facial recognition to a witness, The Post did not count that as independent corroboration, because experts say this process can mislead witnesses into picking “look-alikes” who are not the perpetrator.

If police knew the suspect identified by facial recognition had a tattoo matching that of the person in the surveillance image, The Post counted that as corroboration even if no other steps were taken. If the identity of an AI-recommended suspect was confirmed by a police officer who claimed to have known them from a previous interaction, The Post counted that as corroboration.

Finally, The Post called police departments, prosecutors, defense attorneys and the defendants themselves to learn more about the cases. In some cases, these interviews yielded information that cases were properly corroborated, despite a lack of public documentation.

The 15 police departments that, according to The Post’s analysis, made at least one arrest based on AI results without obtaining independent evidence are:

- Austin
- Bradenton, Florida
- Coral Springs, Florida
- Detroit
- Evansville, Indiana

- Florence, Kentucky
- Jefferson Parish Sheriff's Office, Louisiana
- Maryland Transit Administration Police
- Miami
- Ocala, Florida
- Pflugerville, Texas
- St. Augustine, Florida
- St. John's County Sheriff's Office, Florida
- St. Louis
- Woodbridge, New Jersey

About this story

Editing by Evelyn Larrubia. Emma Talkoff, Jeremy Merrill, Nate Jones and N. Kirkpatrick contributed to this report. Design and development by Emily Wright. Illustration by Lucy Naland. Video editing by Naomi Schanen.

MORE ON FACIAL RECOGNITION



Police seldom disclose use of facial recognition despite false arrests



These cities bar facial recognition tech. Police still found ways to access it.



Eyes on the Cameras, facial recognition public housing

🗨 455 Comments



[Douglas MacMillan](#)

Doug MacMillan is a corporate accountability reporter for The Washington Post. He previously covered technology for the Wall Street Journal, Bloomberg News and Businessweek. X @dmac1

Follow +



[Aaron Schaffer](#)

Aaron Schaffer is a researcher on The Post's News Research team. X @aaronjschaffer

Follow +

The Washington Post

Company

▼

Sections

▼

Get The Post

▼

Contact Us

▼

[About The Post](#)

[Policies & Standards](#)

[Digital Products Terms of Sale](#)

[Print Products Terms of Sale](#)

[Terms of Service](#)

[Privacy Policy](#)

[Cookie Settings](#)

[Submissions & Discussion Policy](#)

[RSS Terms of Service](#)

[Sitemap](#)

[Ad Choices](#)

[washingtonpost.com](#)

© 1996-2025 The Washington Post