The New York Times https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Wrongfully Accused by an Algorithm

In what may be the first known case of its kind, a faulty facial recognition match led to a Michigan man's arrest for a crime he did not commit.

By Kashmir Hill

Published June 24, 2020 Updated Aug. 3, 2020

Note: In response to this article, the Wayne County prosecutor's office said that Robert Julian-Borchak Williams could have the case and his fingerprint data expunged. "We apologize," the prosecutor, Kym L. Worthy, said in a statement, adding, "This does not in any way make up for the hours that Mr. Williams spent in jail."

On a Thursday afternoon in January, Robert Julian-Borchak Williams was in his office at an automotive supply company when he got a call from the Detroit Police Department telling him to come to the station to be arrested. He thought at first that it was a prank.

An hour later, when he pulled into his driveway in a quiet subdivision in Farmington Hills, Mich., a police car pulled up behind, blocking him in. Two officers got out and handcuffed Mr. Williams on his front lawn, in front of his wife and two young daughters, who were distraught. The police wouldn't say why he was being arrested, only showing him a piece of paper with his photo and the words "felony warrant" and "larceny."

His wife, Melissa, asked where he was being taken. "Google it," she recalls an officer replying.

The police drove Mr. Williams to a detention center. He had his mug shot, fingerprints and DNA taken, and was held overnight. Around noon on Friday, two detectives took him to an interrogation room and placed three pieces of paper on the table, face down.

"When's the last time you went to a Shinola store?" one of the detectives asked, in Mr. Williams's recollection. Shinola is an upscale boutique that sells watches, bicycles and leather goods in the trendy Midtown neighborhood of Detroit. Mr. Williams said he and his wife had checked it out when the store first opened in 2014.

The detective turned over the first piece of paper. It was a still image from a surveillance

video, showing a heavyset man, dressed in black and wearing a red St. Louis Cardinals cap, standing in front of a watch display. Five timepieces, worth $3,800, were shoplifted.

“Is this you?” asked the detective.

The second piece of paper was a close-up. The photo was blurry, but it was clearly not Mr. Williams. He picked up the image and held it next to his face.

“No, this is not me,” Mr. Williams said. “You think all black men look alike?”

Mr. Williams knew that he had not committed the crime in question. What he could not have known, as he sat in the interrogation room, is that his case may be the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm, according to experts on technology and the law.

A faulty system

A nationwide debate is raging about racism in law enforcement. Across the country, millions are protesting not just the actions of individual officers, but bias in the systems used to surveil communities and identify people for prosecution.

Facial recognition systems have been used by police forces for more than two decades. Recent studies by M.I.T. and the National Institute of Standards and Technology, or NIST, have found that while the technology works relatively well on white men, the results are less accurate for other demographics, in part because of a lack of diversity in the images used to develop the underlying databases.

Last year, during a public hearing about the use of facial recognition in Detroit, an assistant police chief was among those who raised concerns. “On the question of false positives — that is absolutely factual, and it’s well-documented,” James White said. “So that concerns me as an African-American male.”

This month, Amazon, Microsoft and IBM announced they would stop or pause their facial recognition offerings for law enforcement. The gestures were largely symbolic, given that the companies are not big players in the industry. The technology police departments use is supplied by companies that aren’t household names, such as Vigilant Solutions, Cognitec, NEC, Rank One Computing and Clearview AI.

Clare Garvie, a lawyer at Georgetown University’s Center on Privacy and Technology, has written about problems with the government’s use of facial recognition. She argues that low-quality search images — such as a still image from a grainy surveillance video — should be banned, and that the systems currently in use should be tested rigorously for accuracy and bias.

“There are mediocre algorithms and there are good ones, and law enforcement should only buy the good ones,” Ms. Garvie said.

About Mr. Williams’s experience in Michigan, she added: “I strongly suspect this is not the first case to misidentify someone to arrest them for a crime they didn’t commit. This is just the first time we know about it.”

In a perpetual lineup

In October 2018, someone shoplifted five watches, worth $3,800, from a Shinola store in Detroit. Sylvia Jarrus for The New York Times

Mr. Williams’s case combines flawed technology with poor police work, illustrating how facial recognition can go awry.

The Shinola shoplifting occurred in October 2018. Katherine Johnston, an investigator at Mackinac Partners, a loss prevention firm, reviewed the store’s surveillance video and sent a copy to the Detroit police, according to their report.

Five months later, in March 2019, Jennifer Coulson, a digital image examiner for the

Michigan State Police, uploaded a “probe image” — a still from the video, showing the man in the Cardinals cap — to the state’s facial recognition database. The system would have mapped the man’s face and searched for similar ones in a collection of 49 million photos.

The state’s technology is supplied for $5.5 million by a company called DataWorks Plus. Founded in South Carolina in 2000, the company first offered mug shot management software, said Todd Pastorini, a general manager. In 2005, the firm began to expand the product, adding face recognition tools developed by outside vendors.

When one of these subcontractors develops an algorithm for recognizing faces, DataWorks attempts to judge its effectiveness by running searches using low-quality images of individuals it knows are present in a system. “We’ve tested a lot of garbage out there,” Mr. Pastorini said. These checks, he added, are not “scientific” — DataWorks does not formally measure the systems’ accuracy or bias.

“We’ve become a pseudo-expert in the technology,” Mr. Pastorini said.

In Michigan, the DataWorks software used by the state police incorporates components developed by the Japanese tech giant NEC and by Rank One Computing, based in Colorado, according to Mr. Pastorini and a state police spokeswoman. In 2019, algorithms from both companies were included in a federal study of over 100 facial recognition systems that found they were biased, falsely identifying African-American and Asian faces 10 times to 100 times more than Caucasian faces.

Rank One’s chief executive, Brendan Klare, said the company had developed a new algorithm for NIST to review that “tightens the differences in accuracy between different demographic cohorts.”

After Ms. Coulson, of the state police, ran her search of the probe image, the system would have provided a row of results generated by NEC and a row from Rank One, along with confidence scores. Mr. Williams’s driver’s license photo was among the matches. Ms. Coulson sent it to the Detroit police as an “Investigative Lead Report.”

“This document is not a positive identification,” the file says in bold capital letters at the top. “It is an investigative lead only and is not probable cause for arrest.”

This is what technology providers and law enforcement always emphasize when defending facial recognition: It is only supposed to be a clue in the case, not a smoking gun. Before arresting Mr. Williams, investigators might have sought other evidence that he committed the theft, such as eyewitness testimony, location data from his phone or proof that he owned the clothing that the suspect was wearing.

In this case, however, according to the Detroit police report, investigators simply included Mr. Williams's picture in a "6-pack photo lineup" they created and showed to Ms. Johnston, Shinola's loss-prevention contractor, and she identified him. (Ms. Johnston declined to comment.)

'I guess the computer got it wrong'

The Detroit Detention Center. Mr. Williams was held for 30 hours. Sylvia Jarrus for The New York Times

Mr. Pastorini was taken aback when the process was described to him. "It sounds thin all the way around," he said.

Mr. Klare, of Rank One, found fault with Ms. Johnston's role in the process. "I am not sure if this qualifies them as an eyewitness, or gives their experience any more weight than other persons who may have viewed that same video after the fact," he said. John Wise, a spokesman for NEC, said: "A match using facial recognition alone is not a means for positive identification."

The Friday that Mr. Williams sat in a Detroit police interrogation room was the day before his 42nd birthday. That morning, his wife emailed his boss to say he would miss work

because of a family emergency; it broke his four-year record of perfect attendance.

In Mr. Williams's recollection, after he held the surveillance video still next to his face, the two detectives leaned back in their chairs and looked at one another. One detective, seeming chagrined, said to his partner: "I guess the computer got it wrong."

They turned over a third piece of paper, which was another photo of the man from the Shinola store next to Mr. Williams's driver's license. Mr. Williams again pointed out that they were not the same person.

Mr. Williams asked if he was free to go. "Unfortunately not," one detective said.

Mr. Williams was kept in custody until that evening, 30 hours after being arrested, and released on a $1,000 personal bond. He waited outside in the rain for 30 minutes until his wife could pick him up. When he got home at 10 p.m., his five-year-old daughter was still awake. She said she was waiting for him because he had said, while being arrested, that he'd be right back.

She has since taken to playing "cops and robbers" and accuses her father of stealing things, insisting on "locking him up" in the living room.

Getting help

Mr. Williams with his wife, Melissa, and their daughters at home in Farmington Hills, Mich. Sylvia Jarrus for The New York Times

The Williams family contacted defense attorneys, most of whom, they said, assumed Mr. Williams was guilty of the crime and quoted prices of around $7,000 to represent him. Ms. Williams, a real estate marketing director and food blogger, also tweeted at the American Civil Liberties Union of Michigan, which took an immediate interest.

“We’ve been active in trying to sound the alarm bells around facial recognition, both as a

threat to privacy when it works and a racist threat to everyone when it doesn't," said Phil Mayor, an attorney at the organization. "We know these stories are out there, but they're hard to hear about because people don't usually realize they've been the victim of a bad facial recognition search."

Two weeks after his arrest, Mr. Williams took a vacation day to appear in a Wayne County court for an arraignment. When the case was called, the prosecutor moved to dismiss, but "without prejudice," meaning Mr. Williams could later be charged again.

Maria Miller, a spokeswoman for the prosecutor, said a second witness had been at the store in 2018 when the shoplifting occurred, but had not been asked to look at a photo lineup. If the individual makes an identification in the future, she said, the office will decide whether to issue charges.

A Detroit police spokeswoman, Nicole Kirkwood, said that for now, the department "accepted the prosecutor's decision to dismiss the case." She also said that the department updated its facial recognition policy in July 2019 so that it is only used to investigate violent crimes.

The department, she said in another statement, "does not make arrests based solely on facial recognition. The investigator reviewed video, interviewed witnesses, conducted a photo lineup."

On Wednesday, the A.C.L.U. of Michigan filed a complaint with the city, asking for an absolute dismissal of the case, an apology and the removal of Mr. Williams's information from Detroit's criminal databases.

The Detroit Police Department "should stop using facial recognition technology as an investigatory tool," Mr. Mayor wrote in the complaint, adding, "as the facts of Mr. Williams's case prove both that the technology is flawed and that DPD investigators are not competent in making use of such technology."

Mr. Williams's lawyer, Victoria Burton-Harris, said that her client is "lucky," despite what he went through.

"He is alive," Ms. Burton-Harris said. "He is a very large man. My experience has been, as a defense attorney, when officers interact with very large men, very large black men, they immediately act out of fear. They don't know how to de-escalate a situation."

'It was humiliating'

Mr. Williams and his wife have not talked to their neighbors about what happened. They

wonder whether they need to put their daughters into therapy. Mr. Williams's boss advised him not to tell anyone at work.

"My mother doesn't know about it. It's not something I'm proud of," Mr. Williams said. "It's humiliating."

He has since figured out what he was doing the evening the shoplifting occurred. He was driving home from work, and had posted a video to his private Instagram because a song he loved came on — 1983's "We Are One," by Maze and Frankie Beverly. The lyrics go:

> *I can't understand*
>
> *Why we treat each other in this way*
>
> *Taking up time*
>
> *With the silly silly games we play*

He had an alibi, had the Detroit police checked for one.

Aaron Krolik contributed reporting.

Kashmir Hill is a tech reporter based in New York. She writes about the unexpected and sometimes ominous ways technology is changing our lives, particularly when it comes to our privacy. More about Kashmir Hill