ACLU

NEWS & COMMENTARY

The Computer Got it Wrong: Why We're Taking the Detroit Police to Court Over a Faulty Face Recognition 'Match'

Face recognition technology turns everybody into a suspect and threatens our civil rights.

Jeremy Shur, Student Attorney, University of Michigan Law School Civil Rights Litigation Initiative
Deborah Won, Student Attorney, University of Michigan Law School Civil Rights Litigation Initiative
April 13, 2021

Last year, Detroit police arrested a Black man, Robert Williams, based on a false face recognition match. They held him in a dirty, overcrowded cell for 30 hours — until they realized that "the computer got it wrong." Unfortunately for Williams, it was too late. He had already been arrested in front of his family and missed work because he was in jail for a theft he did not commit. And even after he was freed, Williams still had to hire a lawyer and go to court to defend himself.

Today, the ACLU joins the University of Michigan Law School's Civil Rights Litigation Initiative and the ACLU of Michigan in filing a federal lawsuit charging that the police violated Williams' rights protected by the Fourth Amendment and Michigan's civil rights law. The lawsuit seeks damages and demands that the Detroit Police Department institute policy changes to halt the abuse of face recognition technology.

It is well documented that face recognition technology is deeply flawed. The technology has a disturbing record of racial bias against people of color and other marginalized groups. Many jurisdictions ban its use for that reason, among others. Face recognition is especially unreliable when attempting to identify Black people,

when the photo used is grainy, when the lighting is bad, and when the suspect is not looking directly at the camera. All of these circumstances were present in the photograph that the Detroit Police Department used in its shoddy investigation, and are common in the type of photographs routinely used by police officers around the country when deploying face recognition technology.

Despite the technology's well-known flaws, Detroit police relied on it almost exclusively in their investigation. They did not perform even a rudimentary investigation into Williams' whereabouts during the time of the Shinola shoplifting incident. If they had, they would have realized that Williams was not the culprit — he was driving home from work outside of Detroit at the time the incident took place. Instead, the police asked an individual who was not even at the store to "identify" the culprit in a six-person photo lineup. The individual had no basis for being asked to identify the suspect: She was not a witness to anything except the same grainy image taken from surveillance video that the police already had. Worse still, the identification process was supposed to be a blind procedure in which the officer who conducts it doesn't know who the suspect is to avoid tipping off the witness, but the officer who facilitated it already knew that Williams was the suspect.

After the "witness" falsely identified Williams, the police submitted a faulty and misleading request for an arrest warrant. They did not include the probe image used to generate the faulty face recognition "match," nor did they disclose that the image was blurry, dark, and showed an obstructed, barely-visible face turned away from the camera — impermissible conditions for a face recognition search by even the police department's own standards. They also failed to mention that face recognition technology is known to be faulty under these circumstances. Nor did they disclose that the image of Williams that "matched" with the culprit's was actually his *expired* driver's license, rather than the most current image of him on file with the state. Moreover, the police did not mention that the individual who picked Williams out of the lineup had never actually *seen* the shoplifter in person. And perhaps most egregiously, the police did not explain that both the unknown suspect and Williams are Black, and that face recognition technology is well known to produce significantly higher rates of false matches when used to try to identify images of Black people, as compared to white men.

This violation of the Williams family's rights is a stark example of the dangers of this technology, especially when used by law enforcement against people of color. Government use of face recognition technology not only poses a danger of turning our streets into a surveillance state, but it also threatens integral aspects of our criminal legal system.

The Fourth Amendment guarantees the right to not be searched or arrested without probable cause. When police use face recognition technology to investigate a crime, they are using a flawed, racially biased tool that does not create the "individualized" suspicion required to establish probable cause. Instead, it turns everyone into a suspect by placing us all in the virtual lineup every time the police investigate a crime. So when face recognition technology produces a "lead," police officers and magistrates would be unwise to trust it, especially if the person in the probe image is Black. Had the police officers who arrested Williams taken the time to compare the probe image photo to Williams' appearance, they would have realized that the two individuals were not the same.

Humans, including police officers and judges, have a hard time understanding just how frequently computers make mistakes. That means that, where face recognition technology is involved, judges may be more likely to believe that the officers established probable cause — a dangerous outcome that could lead to untold numbers of false arrests. Anyone who questions whether people will unthinkingly rely on what the computer tells them to do should think about the last time they turned the wrong way because Google Maps told them to do so, even when they knew it was a wrong turn.

The flaws of face recognition technology also seep into the rest of our criminal legal system. Defendants often do not ever find out that they were accused by a computer. Without this knowledge, defendants are denied their constitutional rights to present a complete defense at trial — they cannot point to the flaws of the accusatory computer that led to their arrest or understand how those flaws might infect the subsequent investigation.

Further, even if defendants *do* learn that a computer accused them, they face additional hurdles throughout the system. While defendants are supposed to be given access to information about the flaws of *human* witnesses pursuant to the Supreme Court's decision in *Brady v. Maryland*, they are routinely denied that same information about the flaws of *technological* accusers that serve similar roles in the investigation and prosecution of a crime. Similarly, while defendants are allowed to cross-examine human witnesses at trial under the U.S. Constitution's Confrontation Clause, defendants are often prevented from similarly testing the reliability of computers that produce testimony against them at trial. Police use of face recognition technology is insidious in any context, and its flaws only become more compounded throughout the life of a defendant's criminal case.

Williams' case makes it painfully clear: Face recognition technology turns everybody into a suspect and threatens our civil rights. We cannot allow flawed technology to participate in an already-flawed criminal legal system — especially when an individual's life and liberty are at stake.