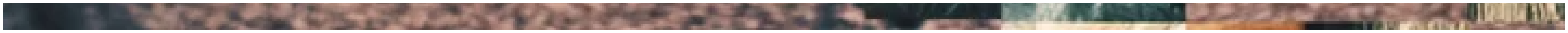
The New York Times https://nyti.ms/2Nkhh6K



How the Police Use Facial Recognition, and Where It Falls Short

Records from Florida, where law enforcement has long used the controversial technology, offer an inside look at its risks and rewards.

By Jennifer Valentino-DeVries

Jan. 12, 2020

After a high-speed chase north of Orlando, Fla., sheriff's deputies punctured the tires of a stolen Dodge Magnum and brought it to a stop. They arrested the driver, but couldn't determine who he was. The man had no identification card. He passed out after stuffing something into his mouth. And his fingerprints, the deputies reported, appeared to have been chewed off.

So investigators turned to one of the oldest and largest facial recognition systems in the country: a statewide program based in Pinellas County, Fla., that began almost 20 years ago, when law enforcement agencies were just starting to use the technology. Officers ran a photo of the man through a huge database, found a likely match and marked the 2017 case as one of the system's more than 400 successful "outcomes" since 2014.

A review of these Florida records — the most comprehensive analysis of a local law enforcement facial recognition system to date — offers a rare look at the technology's potential and its limitations.

Officials in Florida say that they query the system 4,600 times a month. But the technology is no magic bullet: Only a small percentage of the queries break open investigations of unknown suspects, the documents indicate. The tool has been effective with clear images — identifying recalcitrant detainees, people using fake IDs and photos from anonymous social media accounts — but when investigators have tried to put a name to a suspect glimpsed in grainy surveillance footage, it has produced significantly fewer results.

The Florida program also underscores concerns about new technologies' potential to violate due process. The system operates with little oversight, and its role in legal cases is not always disclosed to defendants, records show. Although officials said investigators could not rely on facial recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence.

"It's really being sold as this tool accurate enough to do all sorts of crazy stuff," said Clare Garvie, a senior associate at the Center on Privacy and Technology at Georgetown Law. "It's not there yet."

Facial recognition has set off controversy in recent years, even as it has become an everyday tool for unlocking cellphones and tagging photos on social media. The industry has drawn in new players like Amazon, which has courted police departments, and the technology is used by law enforcement in New York, Los Angeles, Chicago and elsewhere, as well as by the F.B.I. and other federal agencies. Data on such systems is scarce, but a 2016 study found that half of American adults were in a law enforcement facial recognition database.

Police officials have argued that facial recognition makes the public safer. But a few cities, including San Francisco, have barred law enforcement from using the tool, amid concerns about privacy and false matches. Civil liberties advocates warn of the pernicious uses of the technology, pointing to China, where the government has deployed it as a tool for authoritarian control.

In Florida, facial recognition has long been part of daily policing. The sheriff's office in Pinellas County, on the west side of Tampa Bay, wrangled federal money two decades ago to try the technology and now serves as the de facto facial recognition service for the state. It enables access to more than 30 million images, including driver's licenses, mug shots and juvenile booking photos.

"People think this is something new," the county sheriff, Bob Gualtieri, said of facial recognition. "But what everybody is getting into now, we did it a long time ago."

A Question of Due Process

Only one American court is known to have ruled on the use of facial recognition by law enforcement, and it gave credence to the idea that a defendant's right to the information was limited.

Willie Allen Lynch was accused in 2015 of selling $50 worth of crack cocaine, after the Pinellas facial recognition system suggested him as a likely match. Mr. Lynch, who claimed he had been misidentified, sought the images of the other possible matches; a Florida appeals court ruled against it. He is serving an eight-year prison sentence.

Any technological findings presented as evidence are subject to analysis through special hearings, but facial recognition results have never been deemed reliable enough to stand up to such questioning. The results still can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies.

Laws and courts differ by state on what investigative materials must be shared with the defense. This has led some law enforcement officials to argue that they aren't required to disclose the use of facial recognition.

In some of the Florida cases The Times reviewed, the technology was not mentioned in initial warrants or affidavits. Instead, detectives noted "investigative means" or an "attempt to identify" in court documents, while logging the matters as facial recognition wins in the Pinellas County records. Defense lawyers said in interviews that the use of facial recognition was sometimes mentioned later in the discovery process, but not always.

Aimee Wyant, a senior assistant public defender in the judicial circuit that includes Pinellas County, said defense lawyers should be provided with all the information turned up in an investigation.

"Once the cops find a suspect, they're like a dog with a bone: That's their suspect," she said. "So we've got to figure out where they got that name to start."

Law enforcement officials in Florida and elsewhere emphasized that facial recognition should not be relied on to put anyone in jail. "No one can be arrested on the basis of the computer match alone," the New York police commissioner, James O'Neill, wrote in a June op-ed.

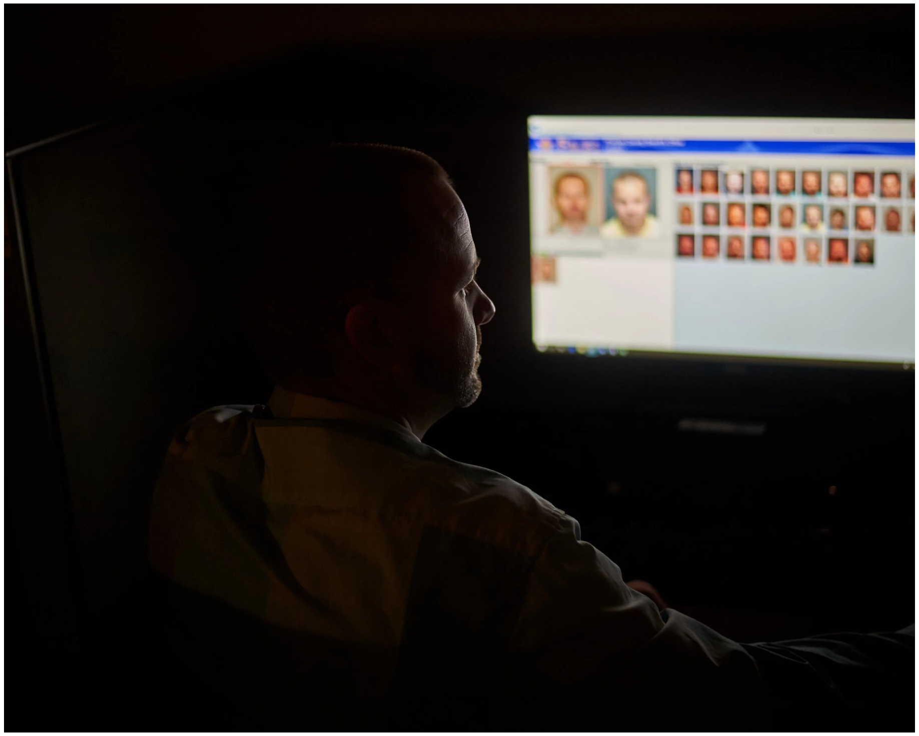
In most of the Florida cases The Times reviewed, investigators followed similar guidelines. But in a few instances, court records suggest, facial recognition was the primary basis for an arrest.

Last April, for example, a Tallahassee police officer investigating the theft of an $80 cellphone obtained a store surveillance image and received a likely match from the facial recognition system, according to the Pinellas list. The investigator then “reviewed the surveillance video and positively identified” the suspect, she wrote in a court document.

A police department spokeswoman suggested that this step provided a check on the facial recognition system. “What we can’t do is just say, ‘Oh, it’s this guy,’ and not even look at it,” she said, adding that in this instance “it was a very clear photo.” The case is proceeding.

No More ‘Name Game’

Pinellas County’s Face Analysis Comparison & Examination System, or FACES, was started with a $3.5 million federal grant arranged in 2000 by Representative Bill Young, a Florida Republican who led the House Appropriations Committee.



Jake Ruberto, a technical support specialist in the Pinellas County Sheriff’s Office, demonstrating the facial recognition system. Zack Wittman for The New York Times

Earlier tests with law enforcement agencies elsewhere had produced meager results, including systems in California that had led to one arrest in four years. Still, the potential was tantalizing. Pinellas’s first planned use for facial recognition was in the local jail’s mug shot system. After Sept. 11, the program was expanded to include the airport. Eventually, sheriff’s deputies were able to upload photos taken with digital cameras while on patrol.

The program received more than $15 million in federal grants until 2014, when the county took over the annual maintenance costs, now about $100,000 a year, the sheriff's office said.

The first arrest attributed to the Florida program came in 2004, after a woman who was wanted on a probation violation gave deputies a false name, local news outlets reported.

The number of arrests ticked up as the system spread across the state and the pool of images grew to include the driver's license system. By 2009, the sheriff's office had credited it with nearly 500 arrests. By 2013, the number was approaching 1,000. Details on only a small number of cases were disclosed publicly.

The latest list, of more than 400 successes since 2014, which The Times obtained after a records request, is flawed: Not all successful identifications are logged, and questionable or negative results are not recorded. Still, together with related court documents — records were readily available for about half the cases — the list offers insights into which crimes facial recognition is best suited to help solve: shoplifting, check forgery, ID fraud.

In case after case on the list, officers were seeking ID checks. "We call it the name game," Sheriff Gualtieri said. "We stop somebody on the street, and they say, 'My name is John Doe and I don't have any identification.'"

In about three dozen court cases, facial recognition was crucial despite being used with poorer-quality images. Nearly 20 of these involved minor theft; others were more significant.

After a 2017 armed robbery at an A.T.M. in nearby Hillsborough County, the Pinellas records show, investigators used facial recognition to identify a suspect. They showed the A.T.M. surveillance video to his girlfriend, who confirmed it was him, according to an affidavit. He pleaded guilty.

Instances of violent crime in which the system was helpful — such as the F.B.I.'s tracking a fugitive accused of child rape — typically involved not surveillance images but people with fake IDs or aliases.

In nearly 20 of the instances on the Pinellas list, investigators were trying to identify people who could not identify themselves, including Alzheimer's patients and murder victims. The sheriff's office said the technology was also sometimes used to help identify witnesses.

The most cutting-edge applications of facial recognition in the area — at the airport, for instance — never showed significant results and were scrapped.

"For me it was a bridge too far and too Big Brother-ish," Sheriff Gualtieri said.

Garbage in, Garbage Out

"It comes down to image quality," said Jake Ruberto, a technical support specialist in the Pinellas County Sheriff's Office who helps run the facial recognition program. "If you put garbage into the system, you're going to get garbage back."

The software for FACES is developed by Idemia, a France-based company whose prototype algorithms did well in several recent tests by the National Institute of Standards and Technology.

But the systems used by law enforcement agencies don't always have the latest algorithms; Pinellas's, for example, was last overhauled in 2014, although the county has been evaluating other, more recent, products. Idemia declined to comment on it.

The gains in quality of the best facial recognition technology in recent years have been astounding. In government tests, facial recognition algorithms compared photos with a database of 1.6 million mug shots. In 2010, the error rate was just under 8 percent in ideal conditions — good lighting and high-resolution, front-facing photos. In 2018, it was 0.3 percent. But in surveillance situations, law enforcement hasn't been able to count on that level of reliability.

Perhaps the biggest controversy in facial recognition has been its uneven performance with people of different races. The findings of government tests released in December show that the type of facial recognition used in police investigations tends to produce more false positive results when evaluating images of black women. Law enforcement officials in Florida said the technology's performance was not a sign that it somehow harbored racial prejudice.

Officials in Pinellas and elsewhere also stressed the role of human review. But tests using passport images have shown that human reviewers also have trouble identifying the correct person on a list of similar-looking facial recognition results. In those experiments, passport-system employees chose wrong about half the time.

Poorer-quality images are known to contribute to mismatches, and dim lighting, faces turned at an angle, or minimal disguises such as baseball caps or sunglasses can hamper accuracy.

In China, law enforcement tries to get around this problem by installing intrusive high-definition cameras with bright lights at face level, and by tying facial recognition systems to other technology that scans cellphones in an area. If a face and a phone are detected in the same place, the system becomes more confident in a match, a Times investigation found.

In countries with stronger civil liberties laws, the shortcomings of facial recognition have proved problematic, particularly for systems intended to spot criminals in a crowd. A study of one such program in London, which has an extensive network of CCTV cameras, found that of the 42 matches the tool suggested during tests, only eight were verifiably correct.

Current and former Pinellas County officials said they weren't surprised. "If you're going to get into bank robberies and convenience store robberies, no — no, it doesn't work that well," said Jim Main, who handled technical aspects of the facial recognition program for the sheriff's office until he retired in 2014. "You can't ask, like: 'Please stop for a second. Let me get your photo.'"

Kitty Bennett contributed research.