The Washington Post

Technology

FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches

A cache of records shared with The Washington Post reveals that agents are scanning millions of Americans' faces without their knowledge or consent.

By Drew Harwell
July 7

Agents with the Federal Bureau of Investigation and Immigration and Customs Enforcement have turned state driver's license databases into a facial-recognition gold mine, scanning through millions of Americans' photos without their knowledge or consent, newly released documents show.

Thousands of facial-recognition requests, internal documents and emails over the past five years, obtained through public-records requests by researchers with Georgetown Law's Center on Privacy and Technology and provided to The Washington Post, reveal that federal investigators have turned state departments of motor vehicles databases into the bedrock of an unprecedented surveillance infrastructure.

Police have long had access to fingerprints, DNA and other "biometric data" taken from criminal suspects. But the DMV records contain the photos of a vast majority of a state's residents, most of whom have never been charged with a crime.

Neither Congress nor state legislatures have authorized the development of such a system, and growing numbers of Democratic and Republican lawmakers are criticizing the technology as a dangerous, pervasive and error-prone surveillance tool.

"Law enforcement's access of state databases," particularly DMV databases, is "often done in the shadows with no consent," House Oversight Committee Chairman Elijah E. Cummings (D-Md.) said in a statement to The Post.

Rep. Jim Jordan (Ohio), the House Oversight Committee's ranking Republican, seemed particularly incensed during a hearing into the technology last month at the use of driver's license photos in federal facial-recognition searches without the approval of state legislators or individual license holders.

"They've just given access to that to the FBI," he said. "No individual signed off on that when they renewed their driver's license, got their driver's licenses. They didn't sign any waiver saying, 'Oh, it's okay to turn my information, my photo, over to the FBI.' No elected officials voted for that to happen."

Despite those doubts, federal investigators have turned facial recognition into a routine investigative tool. Since 2011, the FBI has logged more than 390,000 facial-recognition searches of federal

and local databases, including state DMV databases, the Government Accountability Office said last month, and the records show that federal investigators have forged daily working relationships with DMV officials. In Utah, FBI and ICE agents logged more than 1,000 facial-recognition searches between 2015 and 2017, the records show. Names and other details are hidden, though dozens of the searches are marked as having returned a "possible match."

San Francisco and Somerville, Mass., have banned their police and public agencies from using facial-recognition software, citing concerns about governmental overreach and a breach of public trust, and the subject is being hotly debated in Washington. On Wednesday, officials with the Transportation Security Administration, Customs and Border Protection and the Secret Service are expected to testify at a hearing of the House Committee on Homeland Security about their agencies' use of the technology.

The records show the technology already is tightly woven into the fabric of modern law enforcement. They detailed the regular use of facial recognition to track down suspects in low-level crimes, including cashing a stolen check and petty theft. And searches are often executed with nothing more formal than an email from a federal agent to a local contact, the records show.

"It's really a surveillance-first, ask-permission-later system," said Jake Laperruque, a senior counsel at the watchdog group Project on Government Oversight. "People think this is something coming

way off in the future, but these [facial-recognition] searches are happening very frequently today. The FBI alone does 4,000 searches every month, and a lot of them go through state DMVs."

The records also underscore the conflicts between the laws of some states and the federal push to find and deport undocumented immigrants. Though Utah, Vermont and Washington allow undocumented immigrants to obtain full driver's licenses or more-limited permits known as driving privilege cards, ICE agents have run facial-recognition searches on those DMV databases.

More than a dozen states, including New York, as well as the District of Columbia, allow undocumented immigrants to drive legally with full licenses or driving privilege cards, as long as they submit proof of in-state residency and pass the states' driving-proficiency tests.

Lawmakers in Florida, Texas and other states have introduced bills this year that would extend driving privileges to undocumented immigrants. Some of those states already allow the FBI to scan driver's license photos, while others, such as Florida and New York, are negotiating with the FBI over access, according to the GAO.

"The state has told [undocumented immigrants], has encouraged them, to submit that information. To me, it's an insane breach of trust to then turn around and allow ICE access to that," said Clare Garvie, a senior associate with the Georgetown Law center who led the research.

An ICE spokesman declined to answer questions about how the agency uses facial-recognition searches, saying its "investigative techniques are generally considered law-enforcement sensitive."

Asked to comment, the FBI referred The Post to the congressional testimony last month of Deputy Assistant Director Kimberly Del Greco, who said that facial-recognition technology was critical "to preserve our nation's freedoms, ensure our liberties are protected, and preserve our security." The agency has said in the past that while facial-recognition searches can provide helpful leads, agents are expected to verify the findings and secure definitive proof before pursuing arrests or criminal charges.

Twenty-one states, including Texas and Pennsylvania, plus the District of Columbia, allow federal agencies such as the FBI to scan driver's license photos, GAO records show. The agreements stipulate some rules for the searches, including that each must be relevant to a criminal investigation.

The FBI's facial-recognition search has access to local, state and federal databases containing more than 641 million face photos, a GAO director said last month. But the agency provides little information about when the searches are used, who is targeted and how often searches return false matches.

The FBI said its system is 86 percent accurate at finding the right

person if a search is able to generate a list of 50 possible matches, according to the GAO. But the FBI has not tested its system's accuracy under conditions that are closer to normal, such as when a facial search returns only a few possible matches.

Civil rights advocates have said the inaccuracies of facial recognition pose a heightened danger of misidentification and false arrests. The software's precision is highly dependent on a number of factors, including the lighting of a subject's face and the quality of the image, and research has shown that the technology performs less accurately on people with darker skin.

"The public doesn't have a way of controlling what information the government has on them," said Jacinta González, a senior organizer for the advocacy group Mijente who was particularly concerned about how ICE and other agencies could use the scans to track down immigrants. "And now there's this rapidly advancing technology, with very few guidelines and protections for people, putting all of this information at their fingertips in a very scary way."

The records, which include thousands of emails and official documents from federal agencies, as well as Utah, Vermont and Washington state, show how easy it is for a federal investigator to tap into an individual state DMV's database. While some of the driver photo searches were made on the strength of federal subpoenas or court orders, many requests for searches involved nothing more than an email to a DMV official with the target's

"probe photo" attached. The official would then search the driver's license database and provide details of any possible matches.

The search capability was offered not just to help identify criminal suspects, but also to detect possible witnesses, victims, bodies, and innocent bystanders and other people not charged with crimes.

Utah's DMV database was the subject of nearly 2,000 facial-recognition searches from outside law enforcement agencies between 2015 and 2017 — sometimes dozens of searches a day, the records show. One document from Utah's Statewide Information & Analysis Center coached officers on how to make facial-recognition requests; offered four tips for better facial photographs ("lighting, distance, angle, eyes"); and said the database included "over 5 million Utah driver's license & state identification card photos," about 2 million more than the state's population. State officials did not respond to requests for comment.

Many of the requests for searches in Utah came from local police forces across the country seeking to find suspects who may have traveled to the state, but roughly half the searches came from federal agents, according to a log of the searches. The records do not provide suspect names or say whether cases ended in arrests or convictions.

Washington state's Department of Licensing said that its "facial recognition system is designed to be an accurate, non-obtrusive fraud detection tool" and that the agency does not share use of the system with law enforcement unless compelled by a court order.

Vermont officials said they stopped using facial-recognition software in 2017. That year, a local chapter of the American Civil Liberties Union revealed records showing that the state DMV had been conducting the searches in violation of a state law that banned technology involving "the use of biometric identifiers." The state's governor and attorney general came out against the face-scanning software, citing a need to balance public safety with residents' privacy rights.

In the years before the ban, the records show, Vermont officials ran a number of face scans on driver's license photos at the request of ICE agents. Investigators from a number of federal and local agencies emailed the state's DMV with facial-recognition search requests as they pursued people accused of overstaying their visas, providing false information, stealing from stores or, in at least one case, being part of a "suspicious circumstance."

The officers in some emails would provide descriptions of their targets: One was dubbed a "gypsy … scamming elderly people for money," while another was said to have "VERY LARGE PROTRUDING EARS." In others, DMV officials talked about the face-scanning tool as if it were the kind of awe-inspiring technical marvel most often seen on prime-time cop shows.

In one 2014 email, a police officer in the town of Manchester, Vt., asked a DMV official to scan for a man caught on video "brazenly" stealing. The official forwarded the email to a colleague with a made-for-TV flourish, writing, "Can we play NCIS for this officer?"

Drew Harwell
Drew Harwell is a technology reporter for The Washington Post covering artificial intelligence and the algorithms changing our lives. He joined The Post in 2014 and has covered national business and the Trump companies.
Follow