A mounting attack on democratic rights

FBI and ICE scanning driver's license photos with facial recognition technology

Kevin Reed
10 July 2019

A report in the *Washington Post* this week revealed that the Federal Bureau of Investigation (FBI) and Immigration and Customs Enforcement (ICE) have been using facial recognition software to secretly scan databases of millions of driver's license photos—a violation of basic democratic rights. The federal agencies have been engaged in the program for at least eight years.

According to documents made available to the *Post* by the Georgetown Law Center for Privacy and Technology, the FBI alone has logged more than 390,000 facial recognition searches of federal and state databases since 2011, including the Department of Motor Vehicles (DMV) digital catalog of driver's license photos in at least 21 states.

In Utah, according to the article, the "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," with dozens having returned a "possible match."

The *Post* report says that many of the searches are part of the push to find and deport undocumented immigrants, and "that federal investigators have forged daily working relationships with DMV officials." In states such as Utah, Vermont and Washington, where undocumented immigrants are permitted to obtain full driver's licenses or limited driving privilege cards, "ICE agents have run facial-recognition searches on those DMV databases."

According to 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 latest exposure of widespread use of facial recognition software by federal police agencies is further evidence that the state apparatus is systematically violating basic democratic rights with high-tech surveillance tools. Behind the backs of the public, integrated networks, databases and artificial intelligence technologies are being used to build up a mass of information in the form of digital profiles or dossiers on every citizen. Other recent examples of the increased use of biometric surveillance of the public include:

• A March 9 report by NBC 7 San Diego based on a leaked Customs and Border Protection document showed that dossiers on 59 individuals who were involved in political activity opposed to the Trump administration's immigration policy were gathered from social media accounts and used by the Department of Homeland Security to put a travel ban on the passports of US citizens.

• A June 17 report by the American Civil Liberties Union (ACLU) called "The Dawn of Robot Intelligence" said that the merger of the security camera infrastructure built up over decades with state surveillance "deep learning" and "neural networks" of artificial intelligence are being used to monitor the public 24/7 across the country.

• A hack and subsequent publication on June 14 of the corporate data of DHS contractor Perceptics revealed that facial recognition technology is being utilized by the US government on roadways and border crossings to monitor the traveling public.

• A Georgetown Law Center for Privacy and Technology report called “America Under Watch” revealed that major US cities such as Detroit have secretly built up a facial recognition infrastructure that is monitoring the public in “parks, schools, immigration centers, gas stations, churches, abortion clinics, hotels, apartments, fast-food restaurants, and addiction treatment centers,” and is connected with “databases containing hundreds of thousands of photos, including mugshots, driver’s licenses, and images scraped from social media.”

Facial recognition technology is the marriage of high-resolution video and photographic images with artificial intelligence software. The images on photo IDs or those captured by security cameras in public places such as airports, parks, roadways or businesses—are scanned by the software to assemble a map of key facial geometric relationships.

Among these relationships are the distance between the eyes, the distance from the forehead to the chin or from the nose to the chin. These “facial landmarks”—some systems measure as many as 97 landmarks—are then assembled into a profile known as the “facial signature.” These facial signatures, which are being collected and stored by the millions in government databases, are unique to each individual and a form of biometric data comparable to fingerprints and human DNA.

However, fingerprints and DNA are ostensibly collected by law enforcement according to procedures based on long-established legal principles of “reasonable suspicion” and “probable cause.” In the mass processing and storage of facial signatures by the FBI and ICE derived from state-issued ID photo databases, all such formalities have been dropped. In many cases, requests for searches are made with nothing more than an email from the police agency to a DMV official. Among the providers of advanced facial recognition systems for the law enforcement agencies is Amazon. According to earlier media reports , Amazon’s Rekognition artificial intelligence software is used by the state of Oregon for the purpose of scanning photo databases and matching facial identities, including locating individuals through photos on their social media accounts.

Other reports said that Amazon met with ICE officials and promised to help “target or identify immigrants.” Also, in one of its facial recognition patent applications, Amazon proposed to develop a “database of suspicious persons” that could be integrated with home security technologies and create a “neighborhood-wide surveillance system.”

That these truly Orwellian biometric data gathering techniques are being developed by the tech giants and utilized increasingly by the state intelligence apparatus is a warning to the working class. These revelations represent an escalation of the surveillance of the public that was exposed in 2013 by former NSA contractor Edward Snowden, who leaked documents showing that the US government is electronically storing every phone call and email of the entire population.

The response by congressional Democrats to the facial recognition revelations demonstrates their complicity in what has been going on for many years. Their main criticism is that the use of such methods requires federal government regulation. In fact, the release of the documents by the Georgetown Law center to the *Washington Post* is part of ongoing hearings in Washington, DC aimed at passing congressional legislation that will make such surveillance legal.

The Democratic chairman of the House Committee on Oversight and Reform, Elijah Cummings, glossed over the implications of facial recognition scanning, saying merely, “Law enforcement’s access of state databases is often done in the shadows with no consent.” The same is true for DSA member and Democratic Congresswoman Rashida Tlaib, who responded to the exposure of mass video surveillance in Detroit by saying that she would support federal legislation to regulate its use.