

# US officials utilizing driver's license databases to conduct police searches

Nick Barrickman  
18 June 2013

On Monday, the *Washington Post* reported that photo identification records for over 120 million US citizens are being stored in government databases to be used for police investigations.

“Facial-recognition” technology is currently used in 37 states to supply police investigators with potential suspects. The *Post* states that “[t]he faces of more than 120 million people are in searchable photo databases that state officials assembled to prevent driver’s-license fraud but that increasingly are used by police to identify suspects, accomplices and even innocent bystanders in a wide range of criminal investigations.”

The massive trawling of US citizens’ biometric data is yet another fundamental attack on the Fourth Amendment prohibition against unreasonable searches and seizures. Such information is being accumulated by the state without any connection to individualized suspicion of criminal activity.

The police practice involves collecting an individual’s facial imagery, usually as presented on their photo ID, and cross-checking it against various databases where images may produce a match in a criminal case. The *Post* mentions that police have also made use of the social networking website Facebook so as to access images and submit them to a digital lineup.

There are very few legal oversights to such a process. In order for federal officials to get access to state databases, they merely have to announce that such a search is needed for “law enforcement purposes.”

The consequences of such technology are chilling. Participants at any mass protest, strike or demonstration could expect to have their photo taken and their identity determined by a cross-reference with drivers license databases.

The *Post* cited Laura Donohue, a law professor from Georgetown University: “As a society, do we want to

have total surveillance? Do we want to give the government the ability to identify individuals wherever they are... without any immediate probable cause. A police state is exactly what this turns into if everybody who drives has to lodge their information with the police.”

Moreover, the programs’ own inexact capabilities make it possible for an individual to become falsely implicated if a search should match someone’s face to their own.

Though the technology is still relatively new and unable to identify an individual unless given a fairly clear photo capture, the program can assist in identifying a suspect from a variety of means, including variations of the iris, skin texture, or even one’s particular walking gait. Those pushing the program expect that it could soon be used for identifying individuals out of a crowd, raising the capability for mass policing.

Significantly, facial-recognition technology in its current form was first utilized in the Afghanistan and Iraq wars as a means to suppress mass opposition to the occupation of those countries. These methods are now being transferred back home to the US.

News of the program emerges in the aftermath of the recent Supreme Court decision, *Maryland vs. King*, which ruled that police have the right to collect DNA sample of anyone taken into custody, even before they are found guilty of any crime. This information is likewise stored in massive databases that can be used for other purposes.

The DNA collection program, CODIS (short for Combination DNA Index System), in turn emerged when details of massive illegal government spying on US citizens’ email and phone communications were made public by Edward Snowden, a former-NSA

employee who is currently being witch-hunted by the political establishment. Essentially, authorities are creating a vast database of personal information through a nexus of security programs. From their physical appearance, communications, political affiliations, as well as how their days are spent; nothing is going unrecorded.



To contact the WSWS and the  
Socialist Equality Party visit:

**[wsws.org/contact](https://wsws.org/contact)**