Written by **Joe Wolverton, II, J.D.** on July 2, 2018

# Police Use Massive Facial-recognition Database to ID Capital Gazette Suspect

Law enforcement in Maryland used constitutionally questionable facial-recognition technology to identify the man suspected of killing four reporters and one sales associate at the offices of the *Capital Gazette* newspaper in Annapolis on June 28.

The man charged with the homicides is Jarrod Ramos. Police arriving at the scene of the crime apprehended the 38-year old Maryland native, but he refused to answer questions or in any way cooperate with officers. Ramos carried no identification, either, making identification difficult for authorities.

Now it is law enforcement that isn't cooperating, as the facts of what happened next are not completely known.

Apparently Maryland law-enforcement agents uploaded a photo of Ramos into the state's massive database of photos — the Maryland Image Repository System (MIRS), a database containing more than 10 million driver's license photos and mug shots, according to information released by Georgetown University researchers.

After putting the picture through MIRS, law enforcement received a positive match on a previously uploaded image (it is believed to be a mugshot of Ramos taken after an arrest for harassment, but state officials will not confirm that theory), allowing them to identify Ramos.

According to a story in the *Baltimore Sun*, MIRS works by measuring "the width of a suspect's nose, or the shape of an ear, for instance, against the dimensions of others' faces until the software finds potential matches for investigators to consider."

As for how effective MIRS is at recognition faces among its 10 million-photo database, Maryland state safety officials seemed pleased.

"The Facial Recognition System performed as designed," Stephen Moyer, Maryland's public safety secretary, said in a statement. "It has been and continues to be a valuable tool for fighting crime in our state."

It seems that the database indeed functioned as anticipated in the identification of a suspected murderer. The issue, of course, is whether the technology could be used to identify those not suspected of any crime other than being someone the government wants to watch and track.

Furthermore, the provenance of the pictures in the MIRS database should be disturbing to Marylanders and any other American worried about the growth of the surveillance state and the increasing collection

of images of innocent people without their consent or even their knowledge.

In its report, the *Baltimore Sun* reported that some 6,000 to 7,000 law-enforcement agencies have access to the MIRS database and that during one week it was accessed more than 175 times. That frequency of use and that broad a base of access has led to abuse, according to privacy advocates.

In October 2016, the American Civil Liberties Union sent a letter to the Justice Department citing unwarranted (thus unconstitutional) use of facial-recognition databases around the country to identify people participating in demonstrations protesting police brutality.

"We need to stop the widespread use of face recognition technology by police until meaningful safeguards are in place," said Neema Singh Guliani, ACLU legislative counsel. "Half of all adults in the country are in government face recognition databases, yet the vast majority of law enforcement agencies using this technology lack clear policies, audits to ensure accuracy, and transparency."

In the letter, the ACLU claims that the MIRS system in particular was used to identify people who participated in the march protesting the death of Freddie Gray, the 25-year-old Baltimore man who died while in police custody in 2015.

As indicated in the statement by Guliani, the MIRS database has never been audited, according to the information provided by Georgetown University.

An audit of the system would reveal the exact number of photos stored by the government and whether those images were obtained legally and constitutionally, or without the knowledge or consent of the people whose pictures are stored in the government's computers.

While we wait on an audit, one thing known for certain is that the MIRS database includes photos of everyone who has obtained a new driver's license in Maryland in the last seven years.

Read that again: Every resident of Maryland who has gone to the DMV to get a driver's license — which includes having one's picture taken — has had that picture uploaded to the government's MIRS database for future use in identifying anyone the government wants to track.

Upon receiving a driver's license in Maryland, people are not informed that their photos will not only be put on their license, but will be put into a database controlled by the government and accessible by nearly every law-enforcement agency and officer in the state of Maryland.

What's more, it is believed that the picture of anybody who has ever been arrested in Maryland — even if they were found not guilty of any crime — is uploaded and stored in the MIRS database.

"It's unclear if the [Maryland Department of Public Safety and Correctional Services] 'scrubs' its mug shot database to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent," Georgetown reports.

While the facial-recognition technology may have worked to help identify a suspected killer in the case of Jarrod Ramos, the failure to audit the contents of these databases — in use by law-enforcement agencies in all 50 states — and to erase all photos taken in violation of the Constitution is creating a country where there isn't an unmonitored place in the real or cyber world.

One picture of a car and its passengers, one driver's license photo, one unwarranted wiretap, one unwarranted seizure of a phone record, one search of records of an individual's digital communications is too many. If we are a republic of laws, then government at every level must conform to the Constitution's prohibition on unwarranted searches and seizures.

Written by **Joe Wolverton, II, J.D.** on July 2, 2018

The standard is not whether the surveillance and the images stored in government-controlled databases could be helpful in solving crime. The standard is the Constitution — for every issue, on every occasion, with no exceptions.

Anything less than that is a step toward tyranny.

*Image: Spencer_Whalen via iStock / Getty Images Plus*

# Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.

## What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

## Subscribe