

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051

<http://oversight.house.gov>

### Opening Statement Ranking Member Elijah E. Cummings

#### Hearing on “Law Enforcement’s Use of Facial Recognition Technology” March 22, 2017

Thank you Mr. Chairman, and welcome to all of our witnesses here today.

Let me start by acknowledging that facial recognition technology provides law enforcement officials with an innovative and valuable tool to identify suspects and criminals, which helps keep us all safer. The FBI has told us that this technology helps them identify and apprehend criminals to bring them to justice.

I strongly believe that our law enforcement authorities should have access to the most advanced crime fighting tools available to protect our communities, but serious questions have been raised about the accuracy of facial recognition technology, its disparate impact on certain populations, and its use against law-abiding Americans.

To help our law enforcement authorities do their job as effectively as possible, while at the same time protecting the rights of our constituents, we need to examine these questions head on. So, I am thankful that we are having today’s bipartisan hearing.

There are three key points I would like to address today.

First is the question of accuracy. Last year, the Government Accountability Office (GAO) issued a report with a very significant warning. GAO reported that the FBI has “limited information on the accuracy of its face recognition technology capabilities.” GAO also warned that the FBI did not assess how often these searches “erroneously match a person to the database (the false positive rate).”

This is a big problem. GAO made a series of recommendations, including proposing that the FBI conduct more testing to “help ensure that the system is capable of producing sufficiently accurate search results.” Unfortunately, the Department of Justice disputed the need for more accuracy testing and maintained instead that current testing is adequate.

Second is the question of disparate treatment of some Americans. In 2012, a senior technology expert with the FBI co-authored a study finding that some of the leading algorithms used in face recognition systems were 5% to 10% less accurate on African Americans as compared to Caucasians.

Similarly, on October 18, 2016, the Center on Privacy and Technology at the Georgetown University Law Center issued a report finding that “African Americans are disproportionately likely to be subject to police face recognition.”

According to these reports, if you are black, you are more likely to be subjected to this technology, and the technology is more likely to be wrong.

For these reasons, the Center made a very sensible recommendation—that the FBI simply test its system for racial bias. In response, the FBI claims there is no need to test for racial bias because its system is “race blind.” This response is very troubling. Rather than conducting testing that would show whether or not these concerns have merit, the FBI chooses to ignore growing evidence that the technology has a disproportionate impact on African Americans.

Third is the question of protecting other rights of the American people, including their privacy rights, their civil liberties, and their right to free speech. According to GAO, law enforcement authorities now have the ability to search more than **400 million photos**. There does not have to be a warrant, and there does not even have to be probable cause. They search not only criminal mugshots, but photos of law-abiding citizens that are submitted when they apply for jobs, passports, and even driver’s licenses.

I doubt many Americans realize that when they go down to the DMV to get their driver’s licenses, their photos could be made part of a database that can be searched by the FBI.

The Center on Privacy and Technology estimates that 80% of photos in the FBI’s network of facial recognition searches are people who have never been accused of a single crime.

Last year, the ACLU reported that the Baltimore Police Department used this technology against crowds of people who were protesting police misconduct and the death of Freddie Gray.

Now, I was among those crowds. I engaged in those marches. I worked with community leaders. And I spoke at Freddie Gray’s funeral. But I had no idea that police could have been collecting pictures of me and other law-abiding citizens at the time.

Let me shift the example to make the point a different way. Suppose the NRA organized a march on behalf of gun rights that somehow turned violent. Should police be using facial recognition technology against the marchers? Or should we have standards in place for when law enforcement may or may not use this technology against American citizens?

These are the critical questions we will ask our witnesses today. Thank you, Mr. Chairman.

---

Contact: Jennifer Werner, Communications Director, (202) 226-5181.