

Planned Expansion of Facial Recognition by US Agencies Called 'Disturbing'



By [Julia Conley](#) | [Common Dreams](#)

Digital rights advocates reacted harshly Thursday to a new internal U.S. government report detailing how ten federal agencies have plans to greatly expand their reliance on facial recognition in the years ahead.

The Government Accountability Office [surveyed](#) federal agencies and found ten have specific plans to increase their use of the technology by 2023—surveilling people for numerous reasons including identifying criminal suspects, track government employees' level of alertness, and match faces of people on government property with names on watch lists.

[The report](#) (pdf) was released as lawmakers face pressure to pass legislation to limit the use of facial recognition technology by the government and law enforcement agencies.

Sens. Ron Wyden (D-Ore.) and Rand Paul (D-Ky.) [introduced](#) the Fourth Amendment Is Not for Sale Act in April to prevent agencies from using “illegitimately obtained” biometric data, such as photos from the software company Clearview AI. The company has [scrapped](#) billions of photos from social media platforms without approval and is currently used by hundreds of police departments across the United States.

The bill has not received a vote in either chamber of Congress yet.

The plans described in the GAO report tweeted by law professor Andrew Ferguson, author of “The Rise of Big Data Policing,” are “what happens when Congress fails to act.”

New GAO report on [#FacialRecognition](#) shows what happens when Congress fails to act. Train is rolling down the tracks folks... I don't see federal brakes. [#surveillance](#) <https://t.co/8A8w8MTBf0>

– Andrew G. Ferguson (@ProfFerguson) [August 26, 2021](#)

Six agencies including the Departments of Homeland Security (DHS), Justice (DOJ), Defense (DOD), Health and Human Services (HHS), Interior, and Treasury plan to expand their use of facial recognition technology to “generate leads in criminal investigations, such as identifying a person of interest, by comparing their image against mugshots,” the GAO reported.

DHS, DOJ, HHS, and the Interior all reported using Clearview AI to compare images with “publicly available images” from social media.

The DOJ, DOD, HHS, Department of Commerce, and Department of Energy said they plan to use the technology to maintain what the report calls “physical security,” by monitoring their facilities to determine if an individual is on a government

watchlist is present.

“For example, HHS reported that it used [a facial recognition technology] system (AnyVision) to monitor its facilities by searching live camera feeds in real-time for individuals on watchlists or suspected of criminal activity, which reduces the need for security guards to memorize these individuals’ faces,” the report reads. “This system automatically alerts personnel when an individual on a watchlist is present.”

The Electronic Frontier Foundation said the government’s expanded use of the technology for law enforcement purposes is one of the “most disturbing” aspects of the GAO report.

“Face surveillance is so invasive of privacy, so discriminatory against people of color, and so likely to trigger false arrests, that the government should not be using face surveillance at all,” the organization [told MIT Technology Review](#).

According to the *Washington Post*, three lawsuits have been [filed](#) in the last year by people who say they were wrongly accused of crimes after being mistakenly identified by law enforcement agencies using facial recognition technology. All three of the plaintiffs are Black men.

A federal study in 2019 [showed](#) that Asian and Black people were up to 100 times more likely to be misidentified by the technology than white men. Native Americans had the highest false identification rate.

[Maine](#), Virginia, and Massachusetts have banned or sharply curtailed the use of facial recognition systems by government entities, and [cities across the country](#) including San Francisco, Portland, and New Orleans have passed strong ordinances blocking their use.

But many of the federal government’s planned uses for the technology, Jake Laperruque of the Project on Government Oversight told the *Post*, “present a really big surveillance threat that only Congress can solve.”

Our work is licensed under Creative Commons (CC BY-NC-ND 3.0).
Feel free to republish and share widely.