

The creeping authoritarianism of facial recognition

Taylor Millard

3 March 2022

In an effort to lower crime rates, American law enforcement is pushing to combine facial recognition with expanded video surveillance. Politicians worried about their re-election chances due to a perceived crime wave see the expansion as necessary. It's a sharp swing from 2019 and 2020, when cities like San Francisco and New Orleans were banning or at least enacting limits on facial recognition technology due to privacy concerns.

Now, New Orleans plans to roll back its facial recognition prohibition. The Virginia state senate gave law enforcement a late Valentine's Day gift by passing a facial recognition expansion bill on February 15 — the Democrats who unanimously approved a ban on facial recognition last year suddenly changed their minds, as did five Republicans. New York City wants to expand its facial recognition program to fight gun violence.

Law enforcement has a long history of pining for any tool that might give it some sort of edge, citizen due process be damned. Supporters avow that the technology will help investigators find violent crime suspects, including those involved in the January 6 storming of the US Capitol. OneZero reported in 2020 that Wolfcom promoted its real-time face tracking software as perfect for police organizations looking to quickly identify suspects with outstanding warrants.

These claims are apparently overstated, according to privacy advocates. "Unfortunately, law enforcement will often want to get ahold of any type of shiny new tech, with vendors exaggerating how effective the tech is and downplaying its flaws," according to an email from Project on Government Oversight senior policy counsel Jake Laperruque. "[It's] fairly notorious in this regard."

"For example," Laperruque noted, "Clearview AI advertises its tech to police by literally saying it works just like you see on TV shows like CSI and NCIS; that type of hyperbole would be laughable if it wasn't so dangerous to give police highly inaccurate ideas about how the tech works and how much they can rely on it."

Facial recognition technology remains extremely faulty. Detroit Police Chief James Craig said in 2020 that software developed by DataWorks Plus mismatched identities *95 percent of the time* when used by officers, including in the cases of two wrongful arrests in 2019 and 2020. Wayne County prosecutors apologized following each incident.

More troubling is the case of Nijeer Parks who spent *ten days behind bars* in New Jersey after being falsely flagged by facial recognition technology. Parks' lawsuit blames Clearview AI for the mistaken identity but that's not been confirmed. It is also unknown what photo police used to make the match.

There are questions as to whether police will use the technology to target minorities. Amnesty International believes the NYPD is putting up CCTV cameras with facial recognition technology in minority neighborhoods.

“Our analysis shows that the NYPD’s use of facial recognition technology helps to reinforce discriminatory policing against minority communities in New York City,” said Matt Mahmoudi, a researcher at Amnesty International. “We now know that the communities most targeted with stop-and-frisk are also at greater risk of discriminatory policing through invasive surveillance.”

Let’s not forget that places like China use facial recognition to control their own people. They’re accused of using AI to track Uighur Muslims so they can end up in so-called “reeducation camps.” Jaywalkers and people who ventured outside in their pajamas have been publicly shamed and had their personal information released. Russia tracks its citizens through AI and facial recognition, with 125,000 cameras in Moscow alone.

American law enforcement already uses these kinds of tactics. South Florida police employed facial recognition during a George Floyd protest in 2020. Baltimore may have used it in 2015. Privacy advocates want restraints. “I believe that facial recognition technology poses significant risks to civil liberties,” said Matthew Feeney of the CATO Institute in an email. “Absent tight controls, facial recognition can be used to conduct mass surveillance, leading to infringements on privacy and the stifling of First Amendment-protected activities.”

Feeney believes facial recognition technology remains useful in the right setting. He suggests that law enforcement be limited to databases involving outstanding warrants on violent criminals. Another suggestion involves letting people input information into databases if they believe a family member was a victim of a terrorist attack, an accident, or if a child was abducted. The data would have to be promptly removed if the family requested.

Facial recognition technology still has uses in the private sector. People unlock their phones, gaming consoles, and computers with their faces. The Manchester City soccer club in England considered facial recognition instead of tickets to make it easier for fans to access their home stadium (the plan was abandoned following understandable public backlash).

It’s possible that facial recognition technology can be used safely, so long as people know they’re opting into it and are aware of the potential consequences should the program be hacked. Yet whatever its potential uses, government utilization of this tech should be sidelined.