Facial recognition technology and the US military-intelligence apparatus

Kevin Reed
27 June 2019

On Tuesday, the Oakland City Council Public Safety Committee unanimously approved a resolution banning the use of facial recognition (FR) technology by the city, including by the police department. A full vote of the city council on the resolution is planned for July 16.

If the entire city council adopts the ban, Oakland could become the second city in the US to do so, the first being San Francisco which passed a resolution banning FR on May 14. The Oakland resolution would amend the city's surveillance ordinance, stopping any planned use of FR technology by city departments as well as blocking the use of any information gathered by others using it. The Berkeley City Council is also planning a vote on a facial recognition ban on July 9.

In moving the public safety resolution, Oakland City Council President Rebecca Kaplan, a Democrat, presented the issue as primarily one of racial discrimination. "It has become clearer and clearer that there is a serious and ongoing problem of racial inequity with the implementation of facial recognition technology," Kaplan said.

Although the San Francisco resolution—which was passed by a vote of 8-1—raised the threat that FR poses constitutional rights protected by the First, Fourth and 14th Amendments as well as key sections of the California Constitution, it too contained a nod to identity politics stating, "While surveillance technology may threaten the privacy of all of us, surveillance efforts have historically been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective."

That American city governments are banning FR technologies—while simultaneously attempting to bury the explosive class implications of its use beneath the rubbish of racial, ethnic and gender identity politics—indicates that the level of state surveillance already underway with these tools is vast, and an enormous threat to the democratic rights of all those living in the United States.

Facial recognition is most commonly identified with personal computer and smartphone technologies, such as Apple's Face ID, and for automatically identifying family members and friends in personal photo libraries. However, these consumer-level implementations of FR employ only the most rudimentary capabilities of this ever-present technology.

Facial recognition technology is a form of biometrics, the measurement of the distinctive characteristics used to label and describe individuals such as fingerprints and DNA. These systems integrate the basic principles of facial recognition—the measurement of the relative position, size and shape of the eyes, nose, cheekbones and jaw, for example—with more sophisticated three-dimensional skin texture characterizations, motion video and human behavioral analytics.

The advanced development and implementation of FR is, above all, being driven by the requirements of the military-intelligence apparatus and is connected with the Pentagon war machine and massive domestic surveillance operations of the National Security Agency (NSA) and the Department of Homeland Security (DHS).

Now, for example, the US State Department manages a facial recognition database of 117 million American adults, mostly drawn from driver's license photos. The FBI has also implemented Next Generation Identification—developed by the defense contractor Lockheed Martin—to include facial recognition alongside of fingerprints in its criminal and civil databases.

According to media reports, DHS began in 2017 photographing every passenger at the gate before boarding an airplane and has rolled out the process to 15 US airports since 2018. This program, called "Biometric Exit" is run by Customs and Border Protection (CBP) and is used to cross-reference the images of departing passengers with photos from visa and passport applications.

In March 2017, President Trump issued an executive order to speed up the use of facial recognition identification for "100 percent of all international passengers" in the top US airports by 2021. Since then DHS has been rushing to get the systems up and running to scan the faces of travelers on 16,300 flights per week, or approximately 100 million travelers leaving the US every year—of course, many of them US citizens.

As the report published by the ACLU on June 17 called "The Dawn of Robot Intelligence" explains, the surveillance camera infrastructure constructed over many decades and capturing video images of the public 24/7 is now being married with

powerful artificial intelligence systems. The video content being captured by tens of millions of cameras is being put through "video analytics" software that is increasingly capable of sophisticated learning and connected to other forms of electronic surveillance.

According to the ACLU report, the analytics software now in place claims "the ability to detect things such as loiterers, people moving the wrong direction or intruding into forbidden areas, and the abandonment or removal of objects. They claim the ability to note demographic information about people, such as gender, race, and age, and to collect information such as what clothes they are wearing."

These so-called "deep learning" and "neural network" systems of artificial intelligence (AI) are being trained—with the assistance of the tech monopolies like Google and Amazon—to process and recognize human action and activity, body language, emotion, eye movements in real-time. The ACLU says, "The result is rapid progress in automated video analysis—progress that has brought computers to a point where they are on the cusp of becoming virtual security guards across the world."

While the ACLU report focused primarily on the use of FR and AI for domestic police operations, the US military is developing similar systems for the purposes of warfare. The US Department of Defense's DARPA (Defense Advanced Research Projects Agency) has been developing facial recognition technologies for unmanned air and battlefield purposes with a $2 billion budget to do so.

Although the military is careful to claim that the AI technologies being used "do not capture any personally identifiable information"—especially in the aftermath of Google employees' protest against Project Maven—the use of video analytics for drone-based surveillance is well-developed. The purpose of Project Maven is to automate the analysis of drone video footage to find ostensible threats and objects without human analysts.

For the Pentagon, facial recognition is a "non-contact" method of identifying individuals, search and verification. With the assistance of super high resolution and thermal imaging camera techniques, especially in low light situations, the military can detect the presence of people and also recognize faces from long distances. The combination of AI and FR is also a central aspect of security systems on military bases around the world.

Much of the criticisms of the use of facial recognition systems is based on the argument that they are inaccurate and make too many mistakes. Such objections are often combined with an uncritical acceptance of the justifications made by the surveillance state for using FR while ignoring, or making them primary to, the buildup of a facial recognition database of the entire population that is a direct attack on basic democratic rights.

These arguments are similar to those advanced against CIA rendition, indefinite detention and torture programs on the grounds that these are "ineffective" methods of interrogation. On the one hand, they accept the lies of the military-intelligence establishment about what they are doing and, on the other, the criminal methods continue to be utilized anyway.

Much of the criticisms of facial recognition technologies as enabling racial profiling by the police and other law enforcement agencies are based on research by scientists at the MIT Media Lab published in 2018. Based on a dataset of 1,270 faces, the study showed that the FR software from Microsoft, IBM and Megvii from China was accurate 99 percent of the time when identifying the gender of white men and inaccurate 35 percent of the time when identifying the gender of "darker skinned women."

The essential argument of the study is that FR technologies reinforce the biases that exist within society at large. The problem with this approach—which is a divisive and diversionary argument from the essential questions—is that the software companies simply responded by immediately advancing their technology to improve the accuracy of their systems by 10-fold when it comes to identifying "darker-skinned women."

The build-up of enormous databases of facial and other biometric data of the entire population of the US and other countries is part of the preparations for even greater crimes against humanity abroad than have already been committed over the last quarter century of war in the Middle East and North Africa and the suppression of growing opposition to war and social inequality at home.

These threats cannot be fought on the basis of appeals for the shelving of inaccurate methods or identity politics, which serves to split the working class along racial, ethnic and linguistic lines. The working class can only prepare for the huge battles to come in defense of the most basic democratic rights by organizing its enormous revolutionary strength under the banner of socialist internationalism.