The New York Times https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

San Francisco Bans Facial Recognition Technology

By Kate Conger, Richard Fausset and Serge F. Kovaleski
May 14, 2019

SAN FRANCISCO — San Francisco, long at the heart of the technology revolution, took a stand against potential abuse on Tuesday by banning the use of facial recognition software by the police and other agencies.

The action, which came in an 8-to-1 vote by the Board of Supervisors, makes San Francisco the first major American city to block a tool that many police forces are turning to in the search for both small-time criminal suspects and perpetrators of mass carnage.

The authorities used the technology to help identify the suspect in the mass shooting at an Annapolis, Md., newspaper last June. But civil liberty groups have expressed unease about the technology's potential abuse by government amid fears that it may shove the United States in the direction of an overly oppressive surveillance state.

[Facial recognition technology has stoked controversy over the years. Here's a look back.]

Aaron Peskin, the city supervisor who sponsored the bill, said that it sent a particularly strong message to the nation, coming from a city transformed by tech.

"I think part of San Francisco being the real and perceived headquarters for all things tech also comes with a responsibility for its local legislators," Mr. Peskin said. "We have an outsize responsibility to regulate the excesses of technology precisely because they are headquartered here."

But critics said that rather than focusing on bans, the city should find ways to craft regulations that acknowledge the usefulness of face recognition. "It is ridiculous to deny the value of this technology in securing airports and border installations," said Jonathan Turley, a constitutional law expert at George Washington University. "It is hard to deny that there is a public safety value to this technology."

There will be an obligatory second vote next week, but it is seen as a formality.

Similar bans are under consideration in Oakland and in Somerville, Mass., outside of Boston. In Massachusetts, a bill in the State Legislature would put a moratorium on facial recognition and other remote biometric surveillance systems. On Capitol Hill, a bill introduced last month would ban users of commercial face recognition technology from collecting and sharing data for identifying or tracking consumers without their consent, although it does not address the government's uses of the technology.

Matt Cagle, a lawyer with the A.C.L.U. of Northern California, on Tuesday summed up the broad concerns of facial recognition: The technology, he said, "provides government with unprecedented power to track people going about their daily lives. That's incompatible with a healthy democracy."

The San Francisco proposal, he added, "is really forward-looking and looks to prevent the unleashing of this dangerous technology against the public."

In one form or another, facial recognition is already being used in many American airports and big stadiums, and by a number of other police departments. The pop star Taylor Swift has reportedly incorporated the technology at one of her shows, using it to help identify stalkers.

The facial recognition fight in San Francisco is largely theoretical — the police department does not currently deploy such technology, and it is only in use at the international airport and ports that are under federal jurisdiction and are not impacted by the legislation.

Some local homeless shelters use biometric finger scans and photos to track shelter usage, said Jennifer Friedenbach, the executive director of the Coalition on Homelessness. The practice has driven undocumented residents away from the shelters, she said.

Still, it has been a particularly charged topic in a city with a rich history of incubating dissent and individual liberties, but one that has also suffered lately from high rates of property crime.

The ban prohibits city agencies from using facial recognition technology, or information gleaned from external systems that use the technology. It is part of a larger legislative package devised to govern the use of surveillance technologies in the city that requires local agencies to create policies controlling their use of these tools. There are some exemptions, including one that would give prosecutors a way out if the transparency requirements might interfere with their investigations.

Still, the San Francisco Police Officers Association, an officers' union, said the ban would hinder their members' efforts to investigate crime.

"Although we understand that it's not a 100 percent accurate technology yet, it's still evolving," said Tony Montoya, the president of the association. "I think it has been successful in at least providing leads to criminal investigators."

Mr. Cagle and other experts said that it was difficult to know exactly how widespread the technology was in the United States. "Basically, governments and companies have been very secretive about where it's being used, so the public is largely in the dark about the state of play," he said.

But Dave Maass, the senior investigative researcher at the Electronic Frontier Foundation, offered a partial list of police departments that he said used the technology, including Las Vegas, Orlando, San Jose, San Diego, New York City, Boston, Detroit and Durham, N.C.

Other users, Mr. Maass said, include the Colorado Department of Public Safety, the Pinellas County Sheriff's Office in Florida, the California Department of Justice and the Virginia State Police.

U.S. Customs and Border Protection is now using facial recognition in many airports and ports of sea entry. At airports, international travelers stand before cameras, then have their pictures matched against photos provided in their passport applications. The agency says the process complies with privacy laws, but it has still come in for criticism from the Electronic Privacy Information Center, which argues that the government, though promising travelers that they may opt out, has made it increasingly difficult to do so.

But there is a broader concern. "When you have the ability to track people in physical space, in effect everybody becomes subject to the surveillance of the government," said Marc Rotenberg, the group's executive director.

In the last few years, facial recognition technology has improved and spread at lightning speed, powered by the rise of cloud computing, machine learning and extremely precise digital cameras. That has meant once-unimaginable new features for users of smartphones, who may now use facial recognition to unlock their devices, and to tag and sort photos.

But some experts fear the advances are outstripping government's ability to set guardrails to protect privacy.

Mr. Cagle and others said that a worst-case scenario already exists in China, where facial recognition is used to keep close tabs on the Uighurs, a largely Muslim minority, and is being integrated into a national digital panopticon system powered by roughly 200 million surveillance cameras.

American civil liberties advocates warn that the ability of facial surveillance to identify people at a distance, or online, without their knowledge or consent presents unique risks — threatening Americans' ability to freely attend political protests or simply go about their business anonymously in public. Last year, Bradford L. Smith, the president of Microsoft, warned that the technology was too risky for companies to police on their own and asked Congress to oversee its use.

The battle over the technology intensified last year after two researchers published a study showing bias in some of the most popular facial surveillance systems. Called Gender Shades, the study reported that systems from IBM and Microsoft were much better at identifying the gender of white men's faces than they were at identifying the gender of darker-skinned or female faces.

Another study this year reported similar problems with Amazon's technology, called Rekognition. Microsoft and IBM have since said they improved their systems, while Amazon has said it updated its system since the researchers tested it and had found no differences in accuracy.

Warning that African-Americans, women and others could easily be incorrectly identified as suspects and wrongly arrested, the American Civil Liberties Union and other nonprofit groups last year called on Amazon to stop selling its technology to law enforcement.

But even with improvements in accuracy, civil rights advocates and researchers warn that, in the absence of government oversight, the technology could easily be misused to surveil immigrants or unfairly target African-Americans or low-income neighborhoods. In a recent essay, Luke Stark, a postdoctoral researcher at Microsoft Research Montreal, described facial surveillance as "the plutonium of artificial intelligence," arguing that it should be "recognized as anathema to the health of human society, and heavily restricted as a result."

Alvaro Bedoya, who directs Georgetown University's Center on Privacy and Technology, said that more than 30 states allow local or state authorities, or the F.B.I., to search their driver's license photos.

Mr. Bedoya said that these images are tantamount to being in a perpetual police lineup, as law enforcement agencies use them to check against the faces of suspected criminals. He said that the difference is that an algorithm, not a human being, is pointing to the suspect.

He also said that comprehensive regulation of the technology is sorely lacking. "This is the most pervasive and risky surveillance technology of the 21st century," he said.

Daniel Castro, director of the Center for Data Innovation at the Information Technology and Innovation Foundation, is among those who opposed the idea of a ban. He said he would prefer to see face-recognition data accessible to the police only if they have secured a warrant from a judge, following guidelines the Supreme Court has set for other forms of electronic surveillance.

But proponents of the bans say they are an effort to hit the pause button and study the matter before harm is done. The proposed ban in Somerville, the Boston suburb, was sponsored by a councilor, Ben Ewen-Campen. "The government and the public don't have a handle on what the technology is and what it will become," he said on Tuesday.

Next door in Boston, Ed Davis, the former police commissioner, said it was "premature to be banning things." Mr. Davis, who led the department during the Boston Marathon attack, said that no one in the United States wanted to follow the Chinese model.

But he also sees the potential. "This technology is still developing," he said, "and as it improves, this could be the answer to a lot of problems we have about securing our communities."

Joel Engardio, the vice president of Stop Crime SF, said that he agreed that current facial recognition technologies were flawed, but said that the city should not prohibit their use in the future, if they were improved.

"Instead of an outright ban, why not a moratorium?" Mr. Engardio asked. "Let's keep the door open for when the technology improves. I'm not a fan of banning things when eventually it could actually be helpful."

Kate Conger reported from San Francisco; Richard Fausset from Atlanta and Serge F. Kovaleski from New York. Reporting was also contributed by Natasha Singer and Adeel Hassan in New York.

A version of this article appears in print on , Section A, Page 1 of the New York edition with the headline: Tech-Savvy City Bans a Crime-Fighting Tool: Facial Recognition