MOTHERBOARD
TECH BY VICE

San Francisco Bans Facial Recognition Use by Police and the Government

The technology hub is now the first US city to have issued a moratorium on the invasive spy technology.

By **Sarah Emerson** | May 14 2019, 10:01pm

Image: Justin Sullivan/Getty Images

San Francisco just became the first city in the nation to ban the use of facial recognition technology by police and government agencies.

The decision was approved by the city's Board of Supervisors on Tuesday, with supervisor Catherine Stefani as the only nay.

The moratorium is part of the "**Stop Secret Surveillance Ordinance**," a bill that aims to regulate the use of surveillance technology, such as body cameras and biometric software, in San Francisco. The bill requires agencies to draw up plans for how these technologies will be deployed, and then seek approval from the public and Board of Supervisors.

This means that San Francisco citizens can oppose the use of intrusive devices such as IMSI catchers—devices that capture information about any cell phones in range—**that were used by neighboring Oakland police**, according to previously undisclosed records. It also requires agencies to produce annual reports on how surveillance technologies have been used: whether data was shared and why, their purchase cost, a summary of public complaints, and if the agency contracted with any outside parties.

During the Board of Supervisors meeting Tuesday, several members of the board noted that they "don't know" precisely how many city departments make use of surveillance technologies.

"That is precisely why this legislation is important," Supervisor Aaron Peskin, who sponsored the bill, said during the meeting. "This is attempting to evoke that conversation and to make departments actually have these policies so they aren't casual things."

Under the ordinance, agencies must also submit an inventory of existing surveillance technology to the Committee on Information Technology (COIT), which will publish that information on its website. The Committee will then decide whether those agencies can continue using them or not.

Government use of spy technology "disproportionately harms already marginalized communities," Nathan Sheard, the Electronic Frontier Foundation's grassroots advocacy organizer, **wrote**. "It increases the likelihood that they will be entangled with police, ICE, and other agencies with a history of abuse, bias, and unlawful violence."

The new legislation calls facial recognition technology a threat to civil rights and civil liberties, warning of its propensity to "exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."

A **January study by researchers at MIT** revealed that Amazon's facial recognition software, Rekognition, mistook darker-skinned women for men 31 percent of the time. An **earlier MIT study** exposed racial biases in the facial recognition systems of Microsoft, IBM, and Chinese company Megvii, which were all most accurate when identifying white men.

Privacy experts worry that similar technology, when deployed by authorities, will harm already over-policed Black communities. People in these communities "will likely be overrepresented in mug shot-based face recognition databases" due to existing discrimination by law enforcement agencies, according to **a 2016 study** by the Georgetown Center on Privacy and Technology.

The American Civil Liberties Union (ACLU) of Northern California and other advocacy groups **wrote** the Board of Supervisors in support of the bill this month. The letter, which was signed by 25 groups, cited the Bay Area's history of surveilling marginalized communities in secret and without accountability.

But some groups believe the legislation goes too far in regulating surveillance systems.

It was called "a step backwards for privacy" by the Information Technology and Innovation Foundation (ITIF), a nonprofit DC-based think tank that focuses on technology innovation. "Focusing on technology bans misses opportunities to make communities safer and increase privacy," ITIF vice president Daniel Castro said in a statement.

The bill won't stop businesses and residents from installing their own security

cameras, however. Police can still receive clips from, say, a homeowner's doorbell camera, but cannot request footage that uses facial recognition technology.

Neighborhood watch platforms that encourage people to report petty crimes, such as Neighbors—**a home security social network** run by Ring, which is owned by Amazon—have **facilitated profiling** under the auspices of safety. **Patents made public in 2018** suggest **that Ring** may one day implement facial recognition technology.

"Law enforcement agencies are likely to continue to solicit private security camera and Internet of Things video footage," Tracy Rosenberg, director of Media Alliance, a Bay Area social justice group that has worked on technology issues, said in an email.

The law also subjects official partnerships between neighborhood groups and city agencies to oversight, such as the Union Square Business Improvement District, **which shares footage** from at least 350 cameras downtown with San Francisco police.

That stipulation was necessary "to make sure the city doesn't outsource facial recognition to a third party," said Matt Cagle, an attorney with the ACLU of Northern California. "Community watch groups can continue to do their job while not creating a loophole that allows police departments to use a vendor that sits offsite."

Rosenberg does worry about an uptick in neighborhood surveillance, she said, but is pleased that the bill will stop facial recognition technology from misidentifying people as criminal suspects **in real-time policing**. It's "a way to mitigate some of the worst possible outcomes of NextDoor gone wrong," Rosenberg added.

The bill was helmed by Peskin, and co-sponsored by supervisors Norman Yee, Shamann Walton, Hillary Ronen, and Matt Haney.

"Nothing in this policy prevents third parties from sharing information with law enforcement, but we don't want dangerous or untested technology to proliferate in the shadows, either," Peskin said in an email. "If law enforcement enters into an agreement with a third party for the use of surveillance technology, there will need to be a policy for that use and a public record of that use."

Across the Bay, Oakland will vote later this month to amend its current surveillance technology rules to include a ban on facial recognition technology. According to **the San Francisco Chronicle**, the city already boasts one of the strongest ordinances nationwide around spy technology.

Santa Clara County, Berkeley, Davis, and Palo Alto have also passed legislation that regulates surveillance technology already. Last year, the board of directors of Bay Area Rapid Transit (BART) **voted to adopt** a framework for pursuing surveillance technology after some of its members suggested adding facial recognition software to BART cameras.

"We don't know what's going to be coming down the pipeline in five to ten years,"

Cagle said. “So the ordinance is designed to be future-proof against technologies that watch and track us.”

Caroline Haskins contributed reporting.

This story has been updated to include comment from Supervisor Aaron Peskin.