



April 9, 2019

Mayor London Breed
 Supervisor Norman Yee
 Supervisor Sandra Lee Fewer
 Supervisor Catherine Stefani
 Supervisor Aaron Peskin
 Supervisor Gordon Mar
 Supervisor Vallie Brown
 Supervisor Matt Haney
 Supervisor Rafael Mandelman
 Supervisor Hillary Ronen
 Supervisor Shamann Walton
 Supervisor Ahsha Safai
 San Francisco Board of Supervisors
 City Hall, 1 Dr. Carlton B. Goodlett Place
 San Francisco, California

Re: SUPPORT for the Stop Secret Surveillance Ordinance

Dear Supervisors,

We are a coalition of civil rights organizations writing to express support for the Stop Secret Surveillance Ordinance being considered at the April 15, 2019 meeting of the Rules Committee. This legislation will improve public safety with a straightforward and open process for considering surveillance technology proposals, safeguard against dangerous and biased surveillance practices, and provide the public and Board with a necessary voice in important surveillance decisions affecting the City. We urge you to support this ordinance.

This letter explains the purpose of the Ordinance and how it helps protect the privacy and safety of all San Francisco residents. First, the letter outlines the problems addressed by the Ordinance. Second, the letter explains why the City should prevent the deployment of face surveillance technology that poses a threat to people in San Francisco, regardless of its accuracy. Finally, the letter encourages the Board to ensure that the Sheriff and District Attorney are fully subject to the Ordinance.

1. The Ordinance Ensures Diverse Community Members Are Part of Important Public Safety Decisions

Surveillance technologies such as automated license plate readers, drones, sensor-equipped streetlights, and predictive policing software can collect sensitive personal information about where people go, who they associate with, and even how they feel. All too often, such systems operate out of public view and collect information without the knowledge or consent of residents. When used by public agencies, surveillance technology can fundamentally change the relationship between governments and residents, influencing decisions about who receives a government service, who is monitored and subjected to potentially dangerous encounters with the police, and whether people feel comfortable organizing and engaging in activism. San Francisco should not deploy surveillance technology on its residents without public debate about how these technologies work and their potential harms, and clear guidelines for how the technology can be used.

Public and Board scrutiny of surveillance technology is essential because the impacts of surveillance technology are not equitably distributed – time and again, data collection and processing systems focus their digital gaze on immigrants, people of color, and the poor. As a result, actions taken using this data and errors resulting from flawed data or operator misuse disproportionately impact and potentially harm these communities as well. Without adequate public debate or safeguards to prevent misuse, surveillance technology will harm community members. We know this because it has already happened in San Francisco and the Bay Area.

Many Bay Area police departments have secretly deployed surveillance system without policies to govern their use, provide accountability, and ensure people's safety. This has put immigrant and Black community members in harm's way. Here in San Francisco, SFPD officers held a Black woman at gunpoint outside her car after misusing an automated license plate reader that they operated without an adequate policy to prevent potentially grave mistakes.¹ According to a 2015 report, Oakland police's use of license plate readers was effectively concentrated in low-income and Black communities, perpetuating a long history of over-policing.² In San Jose, police

¹ Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU, May 13, 2014, <https://www.aclu.org/blog/privacy-technology/location-tracking/san-francisco-woman-pulled-out-car-gunpoint-because>.

² Dave Maass, *What You Can Learn From Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.

secretly purchased a drone without meaningfully consulting Muslim community members and other residents who have been targeted by the government for their religious affiliation.³ And in Fresno, the police department used social media surveillance software from a vendor that actively encouraged police to spy on Black Lives Matter activists.⁴

Information about residents in local surveillance systems is also vulnerable to demands by federal agencies such as ICE, who may seek to exploit it to fuel inhumane policies. This is not a hypothetical threat – we recently learned that Immigration and Customs Enforcement has purchased access to a driver location database to which police departments can contribute locally-collected data.⁵ We know that ICE can use that database to assist its efforts to locate and deport community members. The potential vulnerability of local surveillance databases to potential access by agencies such as ICE could threaten San Francisco’s commitment to be a sanctuary city for all residents. This Ordinance would require proposals for such systems to be subject to Board and public scrutiny so that residents are not harmed.

The secretive and unaccountable use of surveillance technology not only harms residents, it damages community trust in local governments.⁶ Other cities have experienced this first hand, such as when Oakland’s City Council faced a public backlash after the public learned about secret plans to build a DHS-funded “Domain Awareness Center” that aggregated surveillance feeds from around the city.⁷ Likewise, when citizens and the Seattle City Council discovered that the police department had acquired drones three years earlier, the ensuing protests led the Mayor to shelve the program, stating that Seattle needed to focus on “community building.”⁸ In both cases, the absence of public debate and a process for elected leaders to evaluate technologies triggered an avoidable public controversy that bred distrust in government and sapped staff time and taxpayer resources.

2. The Ordinance Ensures Democratic Debate and Oversight for Surveillance Technology Decisions

This proposed Ordinance is straightforward and ensures proper democratic debate, transparency, and oversight of surveillance technologies. The Ordinance requires that a city department seeking surveillance technology explain to the public how it works and draft clearly written rules for that specific technology that are designed to protect the public. The Ordinance also requires that the proposal be heard by the Board of Supervisors at a regular public meeting. If the Board approves a new surveillance technology at that meeting, the Ordinance ensures the Board and public will be able to understand and evaluate how it is used through the creation of a simple

³ Thomas Mann Miller, *San Jose Police Department's Secret Drone Purchase: Where's the Accountability?*, ACLU-NorCal, July 30, 2014, <https://www.aclunc.org/blog/san-jose-police-departments-secret-drone-purchase-wheres-accountability>.

⁴ Justin Jouvenal, *The new way police are surveillance you: calculating your threat 'score*, Wash. Post, Jan. 10, 2016, https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.3514f883ceeb.

⁵ Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police for Deportations*, ACLU.org, Mar. 13, 2019, <https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data>.

⁶ A 2014 ACLU of California survey found that at least 90 California communities were in possession of various surveillance technologies, and that public debate rarely occurred when technologies were proposed. *State of Surveillance in California – Findings & Recommendations*, January 2015, https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.

⁷ Brian Wheeler, *Police Surveillance: The US city that beat Big Brother*, Sept. 29, 2016, <http://www.bbc.com/news/magazine-37411250>.

⁸ *Seattle Mayor ends police drone efforts*, USA Today, Feb. 7, 2013, <https://www.usatoday.com/story/news/nation/2013/02/07/seattle-police-drone-efforts/1900785/>.

Annual Report. The Ordinance also ensures that there are written safety measures for existing surveillance technologies already in use.

The Ordinance appropriately requires that the public and democratically-elected Board play a role in evaluating new surveillance technologies before they are acquired or used. And by requiring straightforward safeguards and an annual report, the Ordinance helps ensure community members are not harmed and that the Board fully understands how approved technologies are used. This has produced better outcomes in other Northern California communities with similar laws. Since 2016, Santa Clara County, Oakland, Berkeley, Davis, Palo Alto, and BART have all passed similar ordinances to the one before the Board. On repeated occasions, these communities have come to better decisions about surveillance technology – whether it was Santa Clara’s imposition of safeguards on body cameras or Oakland’s scrutiny of a relationship with a federal “fusion center” – because of the process put in place by their local surveillance ordinance. We urge San Francisco to adopt the same common-sense process for considering new surveillance.

3. The Ordinance Protects San Franciscans from Dangerous and Biased Face Surveillance

We also fully endorse the Ordinance’s prohibition on the use of facial recognition technology by city departments. This is a technology that poses a threat to people of color and would supercharge biased government surveillance of our communities. The use of this technology by government agencies poses a unique threat to public safety and the well-being of people in San Francisco, regardless of the technology’s accuracy. San Francisco should refuse to allow government agencies to acquire or use it for at least three reasons: first, due to flaws in face surveillance systems; second, because such systems are frequently built upon biased datasets; and finally, because face surveillance would supercharge invasive and discriminatory government surveillance, regardless of its accuracy.

The biased algorithms and processes that power face surveillance technology pose a threat to people of color. Multiple tests of this technology indicate it is less accurate for darker-skinned people. Peer-reviewed academic research by researchers at MIT has demonstrated that prominent facial recognition technology products perform more poorly for people with darker skin and women.⁹ Last year, Amazon’s Rekognition face surveillance product misidentified 28 members of Congress as persons in a database of booking photos in a test conducted by the ACLU of Northern California.¹⁰ Of those false matches, 39 percent were people of color, even though people of color only constitute 19 percent of Congress. In practice, an erroneous face surveillance system could misinform and influence a government employee’s decision about how to approach a person, including the decision of whether to use force. These kind of flawed systems should not be used to make decisions about San Franciscans’ lives.

The databases the underlie facial recognition systems are frequently biased as well. Facial recognition systems are commonly connected to databases of mugshot photos. These photos are

⁹ Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81: 1-15, 2018, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, New York Times, Jan 24, 2019, <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html>.

¹⁰ Jacob Snow, *Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future Blog, July 26, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.

then used as a reference point when the system searches for people in the world. But because mugshot databases reflect historical over-policing of communities of color, facial recognition “matching” databases are likely disproportionately made up of people of color. If such systems are connected to officer body cameras or surveillance cameras, these communities may be unfairly targeted simply because they appeared in another database or were subject to discriminatory policing in the past.

Face surveillance will also fuel invasive and discriminatory government surveillance. People should be free to go about their daily lives without the government knowing whether they visit a bar or an abortion clinic, march at a political rally, or attend a religious service. Yet with the flip of a switch, the City could add face surveillance to public CCTV cameras, sensor-equipped smart street lights, or even officer-worn body cameras, creating a citywide surveillance network that could track and recognize residents as they move across town. Face surveillance technology makes it easy for the government to track and store intimate details from our private lives, all with little to no human effort. And like the surveillance systems that came before, the harms will fall hardest on people of color, religious minorities, and immigrants. At a time when public protest is at an all-time high and the federal government is attacking immigrants and activists, San Francisco should refuse to build face surveillance systems that could easily be misused for dangerous, authoritarian surveillance.

Face surveillance will not make the San Francisco community safer and could lead to grave harm. It would chill civil engagement and subject residents and visitors to continuous monitoring and potentially violent contacts with law enforcement if it produces erroneous results. Regardless of accuracy, systems built on face surveillance will amplify and exacerbate historical and existing biases that harm immigrants, religious minorities, activists, and people of color. An identification—whether accurate or not—could cost people their freedom or even lives. San Francisco should refuse to go down this road.

4. The Sheriff and District Attorney Should Be Fully Subject to Democratic Oversight and Not Allowed to Unilaterally Exempt Themselves from the Ordinance

It is essential that the Ordinance protect community members regardless of which City Department possesses or operates the surveillance technology. As written, the Ordinance covers all city officials, departments, boards, commissions, including but not limited to the police department, sheriff’s office, and district attorney. But we are concerned about two provisions in the current draft Ordinance that allow the District Attorney or Sheriff to unilaterally exempt themselves from democratic oversight under the Ordinance by declaring that they are acting in a prosecutorial or investigatory capacity.¹¹ These provisions impose an unacceptable veil of secrecy, both as a matter of public policy, and because they undermine the Board’s supervisory authority under state law.

The Board of Supervisors has an obligation to exercise supervision of the conduct of local departments and officers, including the Sheriff and the District Attorney.¹² Last year the

¹¹ This provision appears in the definition of “City Department” at Chap. 19B1 and at Sec. 19B.2.

¹² By law, the Board possess substantial authority to supervise district attorneys and sheriffs, allocate their budgets, approve county contracts, manage grant funding, request reports, and set rules for the acquisition and use of county property. *See, e.g.*, Cal. Govt. Code. § 25303 (mandating that the Board “shall see that [county officers] faithfully perform their duties...and when necessary, require them to...make reports and present their books and accounts for inspection”); Cal. Govt. Code § 23004(c) (authorizing the Board to enter into contracts on behalf of the county); Cal. Govt. Code § 53701 (authoring the Board to accept grants or loans made available by the federal government to finance public works); Cal. Govt. Code §54202 (declaring that local agencies may adopt policies and procedures governing purchases of supplies and equipment used by the local agency);

California Senate Judiciary Committee specifically recognized the power of Boards of Supervisors to “supervise the official conduct of sheriffs and district attorneys, especially in connection with their management, or disbursement of public funds to procure surveillance technologies.”¹³ The Surveillance Ordinance applies these authorities to the acquisition, use, and oversight of various surveillance technologies.

We urge San Francisco to ensure the District Attorney and Sheriff are fully covered by the Ordinance’s requirements.¹⁴ At a minimum, the Ordinance should mandate that the public and Board be informed and given the opportunity to discuss any efforts by the District Attorney and Sheriff to exempt themselves from the Ordinance.

5. Conclusion

Thank you for your consideration of this essential Ordinance designed to protect public safety and ensure that the Board and community have a voice in decisions about surveillance technology in San Francisco. We look forward to working with the Board to pass and implement this Ordinance. Please let us know if you have any questions.

Sincerely,

ACLU of Northern California
Asian Americans Advancing Justice – Asian Law Caucus
Asian Law Alliance
Centro Legal de la Raza
Coalition on Homelessness
Council on American-Islamic Relations SF-Bay Area
Color of Change
Data for Black Lives
Electronic Frontier Foundation
Faith in Action Bay Area
Freedom of the Press Foundation
Greenlining Institute
Harvey Milk LGBTQ Democratic Club
Indivisible SF
Justice 4 Mario Woods Coalition
National Center on Lesbian Rights
Media Alliance
Lawyers’ Committee for Civil Rights
Oakland Privacy
San Francisco Democratic Socialists of America
San Francisco Public Defender Racial Justice Committee
Secure Justice
SF Latino Democratic Club
Tenth Amendment Center
Transgender Law Center

¹³ California Senate Judiciary Committee Analysis of SB 1186 (emphasis added; quotations omitted), available here: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1186#.

¹⁴A similar ordinance in Santa Clara County accomplishes that by requiring that the Board or a court of law – and not simply the Sheriff or DA acting unilaterally – make a determination that oversight under the ordinance obstructs a sheriff or DA’s prosecutorial or investigatory functions. Santa Clara County Ordinance Code Sec. A40-5, https://library.municode.com/ca/santa_clara_county/codes/code_of_ordinances?nodeId=TITAGEAD_DIVA40SUECCOAF_SA40-5COEXSUTE.