SURVEILLANCE TOOLKIT: SAMPLE COALITION LETTER SUPPORTING A BAN ON GOVERNMENT FACIAL RECOGNITION TECHNOLOGY

The following is a draft coalition letter in support of a ban on a particular surveillance technology. A coalition support letter contains a few key elements: it explains who is in your coalition (you can include partner organizations' logos in the header of the letter), the surveillance technology issue in your community and why it matters, and a short explanation of your strategic goal and why they should support it. Submit your letter to the relevant elected body at least one week prior to the meeting where they will discuss your surveillance issue. The blue text should be customized.

Month ##, 2020

Mayor
Councilmember
Councilmember
Councilmember
Councilmember
Your City Council
Street address
City, CA ZIP

Re: Support for Proposed Ordinance to Prohibit the Acquisition and/or Use of Face Recognition Technology

Dear Honorable Members of the City Council,

We are a local coalition dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance. We write to express strong support for the proposed prohibition on the City's acquisition and use of face recognition technology.

The legislation will safeguard residents against dangerous, invasive, and biased systems that endanger their civil rights and safety. We urge you to adopt the ordinance and position our city at the cutting-edge of municipal technology oversight, joining the ranks of cities from California to Massachusetts that have decided to ensure decisions about advanced surveillance technology are firmly under democratic control. This letter explains several reasons the Council should adopt the prohibition.

1. Face recognition technology grants City departments unprecedented power to identify and continuously monitor residents, amplifying historical bias against communities of color, immigrants, and other vulnerable residents.

Face recognition technology enables the government to automatically track residents' identities, whereabouts, associations, and even facial expressions. Using existing video cameras and officer-worn body cameras promised as a way to keep us safe, government agencies can create unfettered citywide networks that place our communities under continuous surveillance. The powerful and automated nature of face recognition incentivizes the needless expansion of surveillance in our communities. People should not have to fear having their movements and private lives logged in a database simply for walking down the street. Face surveillance will make residents of our city less free. It will also lead to new violations of civil rights.

The harms from face recognition will disproportionately impact communities of color and immigrants. This is because face recognition systems connect to existing surveillance infrastructure and amplify biased policing and enforcement practices already present in these communities. Members of these groups are more likely to be tracked – and subject to government interventions – because they attended a political rally, visited an abortion clinic, or attended a religious service. Face recognition systems risk further criminalizing the lives of people of color and immigrants subject to their surveillance.

Face recognition databases also place the personal information and safety of residents at risk. In the absence of a prohibition, implementing a face recognition system in our City may lead to the creation of a sensitive database featuring the face prints of local residents or the use of a secretive private database, created without the consent of community members. Databases containing the face prints of residents may prove an attractive target for exploitation efforts and demands from agencies like ICE, which has already begun mining state databases using this technology. These sensitive biometric databases are vulnerable not only to such misuse, but also to data breaches. Yet unlike a password or a credit card number, a local resident cannot "reset" his or her face if it is compromised due to a breach of a City database.

2. Face recognition technology's demonstrated inaccuracies and biases threaten the civil rights and safety of residents—especially immigrant communities, communities of color, and women.

Multiple studies of facial recognition technology have concluded that it suffers from significant flaws and bias. In December 2019, the National Institute of Standards and Technology (NIST) released a landmark study of prominent facial recognition algorithms that found Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search. According to a peer-reviewed study by researchers at MIT, face recognition technology products perform poorly for people with darker skin and women. When ACLU ran photos of members of Congress through Amazon's "Rekognition" product last year, we found that 28 members of Congress incorrectly "matched" with mugshot booking photos of arrestees. Of the false matches, 39 percent were people of color, even though people of color make up only 20 percent of lawmakers in Congress.

Our City should refuse to test a technology that even has the potential to arbitrarily treat some local residents differently because of their skin color, sex, or other characteristic. The use of inequitable technology will invite unnecessary encounters with law enforcement, and misinformed decisions about the use of force.

But even when a face recognition algorithm is perfectly accurate, it is still vulnerable to other types of bias that pervade the databases and realities that underlie these systems. For example, since face recognition systems often use mugshot photos for matching purposes—and these mugshot databases reflect the historical over-policing of communities of color—the matching databases used by these systems will frequently overrepresent people of color. Communities of color may be unfairly targeted by the gaze of these systems simply because they appeared in a database and were arrested or subjected to discriminatory policing in the past.

3. Voters overwhelmingly oppose government surveillance based on biometrics.

The proposed prohibition aligns with the will of local constituents. In a poll of likely 2020 California voters, 79 percent of Bay Area respondents opposed the government being able to monitor and track a person using biometric information. This view is held widely across generations, ethnic groups, and political parties, according to the poll.

4. Conclusion

The civil rights and civil liberties cost of facial recognition technology substantially outweigh this technology's theoretical benefits. In summary, we recommend the Council adopt the proposed legislation to protect residents from a technology that is primed for abuse, regardless of its accuracy or rules governing its use.

Sincerely,