



December 14, 2020

Los Angeles Board of Police Commissioners
Commission President Eileen Decker
Commissioner Dale Bonner
Commissioner William J. Briggs, II
Commissioner Maria Lou Calanche
Commissioner Steve Soboroff

Police Commissioners:

We are writing to oppose the Special Order concerning face recognition surveillance that Chief Moore has asked you to approve. This request follows recent revelations that LAPD secretly used face recognition surveillance while lying to the public, claiming it did not use this technology at all.¹ It also comes at a time when cities across California and the U.S. are banning police face recognition.² Los Angeles should follow that example, not reward LAPD for secretly using this harmful technology.

For years the LAPD has misled the public about its widespread use of face recognition. This September, the L.A. Times broke the news that LAPD “has used facial recognition software nearly 30,000 times since 2009,” with “hundreds of officers” running face searches of images from “surveillance cameras and other sources,” including photographs taken “during protests in the city this summer.”³ These revelations came after LAPD “consistently denied having records related to facial recognition, and at times denied using the technology at all.” As recently as summer 2019, LAPD spokesman Josh Rubenstein told the Times: “We actually do not use facial recognition in the Department.” LAPD also refused to disclose its

¹ This policy was introduced in a memo dated December 8, 2020, from Chief Moore to the Police Commission: http://www.lapdpolicecom.lacity.org/120820/BPC_20-0207.pdf.

² In California, police use of facial recognition has been banned in San Francisco (in May 2019), Oakland (July 2019), Berkeley (October 2019), and Alameda (December 2019). The technology has also been banned in Boston, Massachusetts (June 2020), Portland, Oregon (September 2020), and Portland, Maine (November 2020).

³ Kevin Rector and Richard Winton, “Despite past denials, LAPD has used facial recognition software 30,000 times in last decade,” L.A. Times (September 21, 2020), <https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software>.

use of this technology in response to Public Records Act requests filed by reporters and community groups including the Stop LAPD Spying Coalition.⁴

LAPD must not be rewarded for its years of hiding its use of face recognition with a policy normalizing and approving this harmful technology. Face recognition surveillance is a highly dangerous weapon that communities across the country are starting to treat as unacceptable in any form. The California Legislature has already warned about the danger of face recognition surveillance and condemned its use.⁵ Microsoft, Amazon, and IBM – three companies responsible for early development of this technology – announced this year that they would end sales to law enforcement agencies, citing the unique danger of placing face recognition in police hands.⁶ A consensus is emerging that only safe response to this technology is absolute prohibition, akin to bans on use of biological and chemical weapons.

The specific face recognition platform that LAPD uses is among the most dangerous implementations of this technology. This platform was built by DataWorks Plus, a South Carolina company whose face recognition platforms have been banned or criticized in other cities. The same platform was used in San Francisco from 2017 to 2019, when it was outlawed. DataWorks Plus also built the face recognition

⁴ Along with denials of requests by media, LAPD denied CPRA Requests #19-5156 and #19-7474, claiming it had no responsive records regarding specific face recognition systems. LAPD also denied a CPRA seeking “documents relating to its use of face recognition.” Georgetown Law Center on Privacy and Technology, *The Perpetual Lineup: Los Angeles*, <https://www.perpetuallineup.org/jurisdiction/los-angeles>.

⁵ On November 18, 2019, the Legislature declared the following:

Facial recognition and other biometric surveillance technology pose unique and significant threats to the civil rights and civil liberties of residents and visitors.

The use of facial recognition and other biometric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights. This technology also allows people to be tracked without consent. It would also generate massive databases about law-abiding Californians, and may chill the exercise of free speech in public places.

Facial recognition and other biometric surveillance technology has been repeatedly demonstrated to misidentify women, young people, and people of color and to create an elevated risk of harmful “false positive” identifications.

The use of facial recognition and other biometric surveillance would disproportionately impact the civil rights and civil liberties of persons who live in highly policed communities. Its use would also diminish effective policing and public safety by discouraging people in these communities, including victims of crime, undocumented persons, people with unpaid fines and fees, and those with prior criminal history from seeking police assistance or from assisting the police.

California AB-1215, Section 1 (2019-2020).

⁶ Diana Bass, “Microsoft Won’t Sell Face Recognition Software to Police,” *L.A. Times* (June 11, 2020), <https://www.latimes.com/business/technology/story/2020-06-11/microsoft-will-stop-selling-facial-recognition-software-to-police>.

platform used by the Detroit Police Department, which incorporates the same three algorithms used in the Los Angeles platform. Detroit Police Chief James Craig has admitted that this system is wrong about approximately 96% of people it identifies.⁷

The DataWorks Plus system has even caused wrongful prosecutions. This summer, the New York Times reported that the DataWorks Plus system used in Detroit produced “the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm.”⁸ A second example of the same system producing a wrongful prosecution has since emerged.⁹ Both the wrongly prosecuted men were Black. LAPD’s deceit about its use of face recognition means there likely have been cases like this in Los Angeles as well. U.S. Senator Sherrod Brown has raised “concern that DataWorks Plus is assisting in violating the civil liberties of citizens across the nation where [the company’s] facial recognition technology has been deployed — including in Michigan, Pennsylvania, California, South Carolina, and Illinois.”¹⁰

Those examples of wrongful arrests are no surprise. Face recognition software systemically misidentifies people of color, women, trans and nonbinary persons, and youth, putting our communities at greater risk of police violence and abuse. In December 2019, a federal government study of commercially available face recognition systems – including the specific software used in Los Angeles – determined that they falsely identify Black and Asian faces 10 to 100 times more often than white faces.¹¹ Another study by MIT and Stanford University researchers found that face recognition software produced error rates of 0.8% for light-skinned men, compared to 34.7% for dark-skinned women.

While LAPD’s current policy addresses searches of “mugshots,” the Department has long tested dangerous forms of real-time face surveillance on the public. In 2004, LAPD began “experimenting with facial-recognition software” on “a hand-held computer with an attached camera” that officers used to determine who to stop, question, and search on the street.¹² These devices were “donated by their

⁷ Jason Koebler, “Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time,” Vice Motherboard (June 29, 2020), <https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time>.

⁸ Kashmir Hill, “Wrongfully Accused by an Algorithm,” N.Y. Times (June 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.

⁹ Elisha Anderson, “Controversial Detroit facial recognition got him arrested for a crime he didn’t commit,” Detroit Free Press (July 10, 2020), <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>.

¹⁰ Brown Blasts Data Works Plus’ Unreliable Facial Recognition Technology (July 1, 2020), <https://www.brown.senate.gov/newsroom/press/release/brown-blasts-dataworks-unreliable-facial-recognition-technology>.

¹¹ Natasha Singer and Cade Metz, “Many Facial-Recognition Systems Are Biased, Says U.S. Study,” N.Y. Times (December 19, 2019), <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>.

¹² “LAPD studies facial recognition software,” Associated Press (December 27, 2004), <https://www.nbcnews.com/id/wbna6759397>.

developer, Santa Monica-based Neven Vision, which wanted field-testing for its technology.” Even though the devices were “still considered experimental” by Neven Vision, the Rampart Division’s gang unit used them to make more than 20 arrests in late 2004.¹³ LAPD later installed “more than a dozen live-monitored CCTV cameras” in undisclosed locations throughout the San Fernando Valley, with the system “programmed to ID people named on ‘hot lists.’”¹⁴ Analysis by Georgetown University researchers showed that “every person who walks by those cameras has her face searched in this way.”¹⁵

LAPD might claim that its proposed policy creates rules for the Department’s otherwise unregulated use of face recognition. This is a problem of LAPD’s own creation, and the only safe way to confront this dangerous technology is an absolute ban, like many other cities have implemented. No rules, reporting, transparency, or criteria can make the use of face surveillance acceptable. Unless we stop the spread of this technology, it will inevitably be used to monitor the faces of every person moving around in public.

We need to keep Los Angeles safe from this dangerous technology, not allow LAPD to continue experimenting on and harming our communities. We therefore demand that the Police Commission:

1. Reject LAPD’s proposed “Use of Photo Comparison Technology” policy.
2. Implement an outright ban on LAPD use of face recognition surveillance.
3. Investigate LAPD’s past use of face recognition surveillance, to understand how the community has been impacted.

Sincerely,

Stop LAPD Spying Coalition
Black Lives Matter - Los Angeles
Los Angeles Community Action Network
White People for Black Lives

¹³ “Mobile Identity Verification System Proven Effective at LAPD’s Rampart Division,” Business Wire (February 7, 2005), <https://www.businesswire.com/news/home/20050207006034/en/Mobile-Identifier-Facial-Recognition-System-Successfully-Deployed-by-LAPD-to-Improve-Neighborhood-Safety>.

¹⁴ Darwin Bond-Graham, “Forget the NSA, LAPD Spies on Millions of Innocent Folks,” LA Weekly (February 17, 2014), <https://www.laweekly.com/forget-the-nsa-the-lapd-spies-on-millions-of-innocent-folks/>.

¹⁵ Georgetown Law Center on Privacy and Technology, The Perpetual Lineup, <https://www.perpetuallineup.org/findings/deployment>.