August 1, 2019

By first-class mail and
by email to bopc@detroitmi.gov

Commissioner Lisa Carter, Chair
Commissioner Darryl D. Brown
Commissioner Evette Griffie
Commissioner Shirley A. Burch
Commissioner Willie E. Bell
Commissioner Willie E. Burton
Commissioner William M. Davis
Commissioner Elizabeth Brooks
Commissioner Rev. Jim Holley, PhD
Commissioner Eva Garza Dewaelsche
Commissioner Annie Holt
Detroit Board of Police Commissioners
1301 Third Street, Suite 767
Detroit, MI 48226

Re: Detroit Police Department's Proposed Policy Governing Use of Facial Recognition Technology

Dear Commissioners,

We write, as a coalition of leading grassroots, civil rights and civil liberties organizations in Detroit and the State of Michigan, to express our deep concern with the use of facial recognition

technology by the Detroit Police Department (DPD). We urge this Commission to vote to reject the facial recognition policy proposed by the DPD on July 25.

Facial recognition technology is flawed and dangerous, and its use in any form by the DPD can serve only to further erode trust between the DPD and Detroiters—especially Detroiters of color. Detroit and the DPD should invest their time and resources in improving community relations and in making real changes in our neighborhoods to improve public safety rather than in finding new ways to use technology to police our neighborhoods from afar. If this Commission approves a policy permitting the DPD's use of facial recognition technology, such a decision threatens to turn Detroit into a national "leader" in surveilling its own residents. Instead, we should be following the lead of cities such as Somerville, Massachusetts, and Oakland and San Francisco, California—communities that have acted promptly and boldly to ensure that facial recognition technology does not gain a foothold in their jurisdictions.[1]

Our concerns about the use of facial recognition in Detroit largely fall into two categories: (1) the disparate impact that the use of such technology will have in communities of color and immigrant communities and (2) the fact that the availability and use of facial recognition technology constitutes an overwhelming threat to the privacy rights not just of Detroiters themselves but of anyone who visits or passes through Detroit.

Facial Recognition Is a Threat to Communities of Color and Immigrant Communities

The harms from the use of facial recognition technology will, inevitably, have a disproportionate impact on communities of color and immigrant communities. These communities already experience racially biased policing and enforcement practices. Facial recognition represents a dangerous new tool that will further contribute to over policing—and the wrong *type* of policing—in our communities.

It is now clear that facial recognition technology performs particularly poorly at identifying individuals of color and women. That was the conclusion of a recent peer-reviewed study by researchers at MIT, discussing the ways that facial recognition technology "discriminate[s] based on classes like race and gender."[2] Similarly, the ACLU recently ran photos of members of Congress through Amazon's "Rekognition" facial recognition product and 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.[3] False identifications of this nature can give rise to unnecessary civil rights violations and serious harms, including wrongful arrests or investigations that can cause lasting damage to individuals' lives even if they are not actually

---

[1] Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, San Francisco Chronicle (July 17, 2019), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

[2] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Machine Learning Res. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[3] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots* (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

charged or are ultimately exonerated. Allowing discriminatory facial recognition technology to operate in a majority Black city will exacerbate all the racial bias already pervading police practices in Detroit. A city like ours should be taking the lead in *resisting* the use of racially biased surveillance technology—not serving as one of its leading proponents.

The existence of facial recognition technology in Detroit is a particularly grave threat to our immigrant communities. Federal agencies like ICE and Customs and Border Patrol (CBP) have exploited state facial recognition tools to target immigrant communities for enforcement actions.[4] Immigrant communities in Detroit, as elsewhere in our state and nation, live in fear of the brutal enforcement methods being pursued at a national level by these agencies. The use of facial recognition technology in Detroit is sure to fray the trust between such communities and law enforcement officials. As this Commission knows, building such trust is vital to the safety of all communities in and around Detroit, and building it is a delicate and time-consuming task. The Commission should recognize that, once lost, such trust is difficult to reclaim.

Indeed, the underlying issue here is one of trust and of wise resource allocation. There is no question that trust between the police and many residents of Detroit's most distressed neighborhoods is frayed. The solutions involve shifting city resources toward better supporting the health and well-being of our residents and their neighborhoods, rather than increasing the level of law enforcement methods used against members of our community. They also involve reinvestment in our city through community building, improving housing and public transportation, addressing public health needs, including access to affordable water, and other measures to help the well-being of residents and the vitality of our neighborhoods. The use of facial recognition as a police tactic accomplishes exactly the opposite. It sends a message that the only way to keep us safe is by treating us as threats to be monitored, tracked, and incarcerated, using ever-more-sophisticated technology. This approach is as counterproductive for accomplishing the goal we all share of building safe communities as it is wasteful of millions of dollars that could be better spent on community reinvestment.

Facial Recognition Poses a Unique Threat to Our Privacy

The facial recognition technology that the DPD has already purchased gives the DPD truly terrifying capabilities. In 2016, the City purchased software and services from DataWorks Plus worth over $1 million. The contract specifically states that DataWorks Plus will provide the City with "FACE Watch Plus real-time video surveillance facial recognition and FACE Plus facial recognition solution" and "will work with the City of Detroit to fine-tune the specifications and create a customized solution that meets our exact needs." The purchase contract includes screening software that "monitors 100 concurrent video feeds" as well as "mobile facial recognition licenses" for an "unlimited" number of users.[5] Thus, the DPD has the capacity to apply its facial recognition technology on a massive scale by combining live video feeds and countless mobile devices operated by individual officers on the ground.

---

[4] Catie Edmonson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. Times (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

[5] *See* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Law Center on Privacy & Technology, at note 11 and cited documentation (May 16, 2019), https://www.americaunderwatch.com/

To use its facial recognition technology, the DPD taps into the Michigan State Police's Statewide Network of Agency Photos (SNAP) database. That database not only contains mugshot photos but also includes over 40 million driver's license and ID photos from the Michigan Department of State. The Department of State has been sharing identity photos with the Michigan State Police for over 20 years without advising Michiganders that by the simple act of acquiring a state ID, they were subjecting themselves to being included in a police photo database that is now being used for facial recognition. In our experience, most Michiganders and Detroiters are dismayed to learn that they are included in such a database. Even so, when the database began in 1998, it could not have been used for mass surveillance of the public because the technology to do so did not exist. Now, with Detroit's acquisition of real-time facial recognition technology, the database has become a far more dangerous tool for mass profiling of Michiganders and a threat to our constitutional liberties. The database is also expanding at an alarming rate, with the Michigan State Police adding around 2.7 million photographs to the database just last year, including photographs culled by law enforcement from Michiganders Facebook accounts and other internet sources.[6]

The combination of these facial recognition capacities means that DPD has the technology to implement mass, pervasive monitoring in our communities. Through the Green Light Program, DPD already has access to over 500 live video feeds that monitor everyone who comes and goes from hundreds of locations throughout the city including medical clinics, sorority houses, churches, schools, hotels, day care centers, and residential apartment communities. When this video capacity is combined with the DataWorks software and the comprehensive SNAP database, DPD can monitor the daily comings and goings of Detroiters as well as anyone working in or visiting the City in ways that would intrude into the deepest corners of our private lives and threaten our Fourth Amendment right to be free from governmental tracking of our personal lives and whereabouts.[7]

We appreciate that the DPD's current policy proposes not to use many of the surveillance capacities that it has already purchased. But the limitations the DPD now suggests it might be willing to accept are in significant tension with its decision to purchase technology with such sweeping capabilities in the first place. It is also in tension with the fact that the DPD began using its facial recognition technology after acquisition without first submitting to oversight by this Commission (or anyone else) for well over a year now. Indeed, even when DPD finally *did* come to this Commission to propose a policy guiding its use of facial recognition technology, the policy it originally proposed would have allowed DPD to surveil First Amendment activities such as political protests or marches under certain conditions.[8] That alarming provision has now

---

[6] Hannah Ball, *Michigan Drivers Info Automatically Put Into Police Database*, Tri-County Times (Mar. 17, 2019), https://www.tctimes.com/news/michigan-drivers-info-automatically-put-into-police-database/article_dcc13de8-4745-11e9-9f20-73a92afa0f89.html.

[7] The Supreme Court recently held that it is unconstitutional to track an individual's "physical movements as captured through" surveillance technology without a warrant. *Carpenter v. United States*, 138 S. Ct. 2206 (2018). In *Carpenter* the issue was whether the government could use cell phone location data to reconstruct an individual's whereabouts without first obtaining a warrant. The Court explained that it was unlawful, without a warrant, to use tracking technology to "reconstruct a person's movements" by essentially "travel[ing] back in time to retrace a person's whereabouts" particularly because the technology "runs against everyone"—not just against a suspect in a criminal case. The same would be true of deploying widespread facial recognition technology throughout the City of Detroit to Green Light Camera feeds, as the DPD is now capable of doing.

[8] That is precisely what happened in Baltimore where facial recognition technology was used to monitor protestors who were protesting police violence against Black civilians. Kevin Rector & Alison Knezevich, *Maryland's Use of*

(thankfully) been removed from DPD's proposed policy. Nonetheless, the history just described demonstrates how easily law enforcement officials can succumb to the allure of using facial recognition technology in insidious ways and without going through democratic channels.

We therefore urge this Commission to vote to deny the DPD the ability to deploy facial recognition technology in any form. Allowing facial recognition technology today sows the seeds of the surveillance state of tomorrow. We implore you to act now before these seeds can grow into something we can no longer uproot.

Sincerely,

Arab American Civil Rights League (ACRL)
Rula Aoun, Director

Arab Community Center for Economic and Social Services (ACCESS)
Hasan Jaber, Executive Director

ACLU of Michigan
Dave Noble, Executive Director, Rodd Monts, Campaign Outreach Coordinator,
Phil Mayor, Senior Staff Attorney

CAIR Michigan
Dawud Walid, Executive Director

Color Of Change
Rashad Robinson, President

Detroit Community Technology Project
Tawana Petty, Data Justice Director

Detroit Hispanic Development Center
Angela Reyes, Executive Director

Detroit Justice Center
Amanda Alexander, Executive Director

Michigan Immigrant Rights Center
Susan E. Reed, Managing Attorney

Michigan United
Ryan Bates, Executive Director

Metropolitan Organizing Strategy Enabling Strength (MOSES)
G. Ponsella Hardaway, Executive Director

We The People - Michigan
Art Reyes III, Executive Director

Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates, The Baltimore Sun (Oct. 18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.