BALTIMORE POLICE DEPARTMENT

Brandon M. Scott
Mayor

Michael S. Harrison
Police Commissioner

February 23, 2021

Honorable President and Members of the Baltimore City Council
Room 400, City Hall
100 N. Holliday Street
Baltimore, Maryland 21202

RE: City Council Bill# 21-0001
Surveillance Technology in Baltimore

Dear Council President Mosby and Members of the City Council:

The Baltimore Police Department (BPD) has reviewed Council Bill #21-0001. This bill seeks to prohibit Baltimore City government from purchasing or obtaining certain face surveillance technology; prohibits Baltimore City government from contracting or subcontracting with another for the purpose of face surveillance technology; prohibits any person in Baltimore City from obtaining, retaining, accessing, or using certain face surveillance technology or any information obtained from certain face surveillance technology requires the Director of Baltimore City Information and Technology to submit an annual report to the Mayor and City Council regarding the use of surveillance by the Mayor and City Council; and provides for a sunset date for certain penalties.

At a time when residents, visitors and business leaders alike are concerned about the crime rate and BPD's ability to solve and ultimately close cases, we should all be supporting innovative investigative techniques that could help make Baltimore a safer city. Although we believe that this bill is well intentioned and borne out of sincere goal of eliminating any real or perceived bias, the Department strongly believes that there are more strategic methods of achieving this objective and that systemic changes could be made to provide overall transparency and vital accountability.

Therefore, the Department opposes this bill in its current form and makes a number of recommendations as to language that should be added in order to meet the Sponsor's goal of fair and impartial investigations and responsible use of technology.

As currently written, this bill would permit the continued use of the Maryland Image Repository System (MIRS), established and maintained by the Maryland Department of Public Safety and Correctional Services (DPSCS), to generate investigative leads that contribute to the closure of all sorts of crimes including but not limited to sex trafficking, carjacking, and murder. MIRS is facial recognition software that is the functional equivalent of a digitized mug shot book. Using MIRS, law enforcement officers throughout the state, who are NCIC certified, are able to compare images of unidentified suspects to images from motor vehicle records and state and FBI mugshots of known offenders.

Although the bill allows the use of this technology that the Department currently relies upon to serve as a force multiplier to aide good old-fashioned investigative work, it completely eliminates the possibility that the Department could acquire more effective technology as it becomes available. We believe that rather than a **prohibition** against the acquisition of any new facial recognition technology, it would be more prudent to establish safeguards to prevent intentional misuse and to reduce the possibility that an innocent individual could suffer from negative consequences.

To that end, we suggest following amendments:

1. Amend page 2, lines 22 and 23 to read as follows: Any agency, department or instrument of Baltimore City government that purchases or otherwise obtains a face surveillance system or face surveillance system must comply with the below listed requirements:

    a. Establish clear policies for each type of application that articulates:
        i. Who is authorized to use the technology; and
        ii. Under what circumstances and with what level of human oversight the technology is to be used.

    b. Post established policies on the agency's website for increased transparency.

    c. All users of facial recognition technology must receive mandatory training that includes but is not limited to the history of the technology, the purpose of the established policy, agency standard operating procedures, data protection, video image extraction techniques, image enhancement regulations, acceptable use, prohibited use and the impact and consequences of policy violations.

    d. The Agency shall conduct annual audits on the use of the technology and post the findings on the Department's website.

2. We also respectfully request that § 41-4 (B)(3)(II) on page 2 be amended to read as follows:

(II) Exclusions.
"Face surveillance system" does not include the following:
(a) A biometric security system designed specifically to protect against unauthorized access to a particular location or an electronic device;
(b) Automatic License Plate Readers (LPRS);
(c) Closed-Circuit Television Cameras;
(d) Gun Shot Detection Hardware and Services; or
(e) Body Worn Cameras (BWC)

It is important to note that although the Law Department has maintained that the City Council does not have the authority to legislate mandates of the Baltimore Police Department, the Department would voluntarily agree to comply with the requirements as listed above and to include in any subsequent policy, the following provisions:

i. In accordance with the Mayor's Executive Order from July 2019 on Advancing Public Safety and Access to City Services and BPD policy #1021, any information obtained through the use of this technology is not to be shared with U.S. Immigration and Customs Enforcement (ICE) in furtherance of civil immigration enforcement efforts;

ii. The SAO office will be notified whenever an arrest was assisted by the use of facial surveillance system technologies;

iii. In accordance with BPD policy #824, Body Worn Camera data shall not be used to create a database or pool of mug shots; be used as fillers in photo arrays or be searched using facial or voice recognition software. BPD is permitted to use facial recognition software to analyze the recording of a specific incident when a supervisory member has reason to believe that a specific suspect, witness or person in need of assistance was recorded;

iv. Constitutional limitations apply to facial recognition deployments. As such, the technology is never to be used in violation of an individual's constitutional rights under the First, Fourth and Fourteenth Amendments, such as surveillance based solely on:

1. Religious, political or social views or activities.
2. Participation in lawful events.
3. The race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation or other classification protected by law against discrimination.

We do want to raise a few items of note. First, in establishing policy, training and audits as discussed above, the BPD is required to collaborate with the Department of Justice, the Monitoring Team, the public and members of the Department to develop those items. While that is a public process, it is not a quick process and would, therefore, take some time for the policies, trainings and audits to be adopted.

Second, the Department's federal Consent Decree also mandates that prior to the deployment of any new technology, the Department is required to notify the public in a timely manner. In addition, the Department has made a habit of seeking approval by the Monitoring Team and the Department of Justice prior to acquisition.

Thank you for allowing BPD to comment on such an important legislative matter.

Sincerely,

Michelle Wirzberger, Esq.
Director of Government Affairs

cc: Natwana Austin, Executive Secretary of the Baltimore City Council
Natasha Mehu, Director of Mayor's Office of Government Relations
Nina Themalis, Special Assistant and Legislative Liaison, MOGR
Brittany Lewis, Chief of Government Affairs, Office of the Council President
Eric Melancon, BPD Chief of Staff
Andrew Smullian, BPD Deputy Chief of Staff