June 10, 2020

The Honorable Kim Janey
City Council President (District-7)
City of Boston, City Council
1 City Hall Square
Room 550
Boston, MA 02201-2043

Dear City Council President Janey:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with the proposed ordinance banning facial recognition technology in Boston, which would prohibit any city government official from utilizing facial recognition technology or any information obtained using the technology.

SIA is a nonprofit trade association representing businesses providing a broad range of security products and services across the U.S., including more than 23 companies headquartered or with major operations centers in the Greater Boston metropolitan area. SIA represents many of the leading developers of facial recognition technology as well as companies offering products that incorporate this technology for a wide variety of security and public safety applications.

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Facial recognition technology offers tremendous benefits to citizens when used effectively and responsibly. Addressing concerns about public sector applications of this technology can and should be accomplished through policies ensuring appropriate transparency, procedures, and oversight. We believe that eliminating the potential benefits to Bostonians by completely banning its use is premature.

Unlike many of the criticisms, the benefits of facial recognition are not potential or hypothetical – they are proven and growing. In the U.S., the technology has been used for over a decade to detect identity fraud against state programs that also fuels other criminal activity. It also been used to help find and rescue human trafficking victims, thwart potential terrorist attacks, solve hate crimes against the LGBTQ community and crack cold cases. Despite media reporting on accuracy concerns at the algorithm level (versus full operational systems used in conjunction with policies, procedures and appropriate human review), law enforcement agencies in the U.S. have a decade-plus operating history of many thousands of instances of successful use as a tool to increase the speed and accuracy of investigations.[1]

These proven and beneficial uses of facial recognition are not "surveillance", yet "*face surveillance*" as mislabeled and banned in the proposal, encompasses all facial recognition technology with few exceptions. One exception is authentication to access personal electronic devices. Yet there are other uses where similarly there is little privacy or civil liberties concern, often where there is already consent or an existing requirement to prove one's identity. This includes access control to secure areas of buildings, and other security measures protecting employees and visitors to government facilities. Despite extremely varied privacy considerations depending on the application**, s**uch non-controversial uses are also included in the blanket ban as currently written.

[1] https://www.securityindustry.org/advocacy/policy-priorities/facial-recognition/

Lastly, modern facial recognition technology is highly accurate. Proper context is needed for discussions about error rates – while no biometric identification technology is 100% accurate, facial recognition accuracy is reaching that of automated fingerprint comparison, which is generally viewed as the gold standard for identification. The National Institute of Standards and Technology (NIST), the world's leading authority on facial matching technology, has concluded that the software it tests is 20 times better[2] at searching a database to find a matching picture than it was in 2014, and a NIST report last year recorded "close to perfect" results with miss rates averaging just 0.1 percent for the most accurate systems.

Related to this, a key misconception driving the justification for the proposal involves the alleged risks and implications of "misidentification" by the technology. Here it is important to point out that in any process where there are potential high-consequence outcomes, such as law enforcement investigations, there are no automated decisions made solely by the technology. In these cases, the technology serves only as a tool to assist personnel, who ultimately must use other means to verify an identification.

Limiting variation in performance across demographic groups is critically important. Again, context is critical, as image quality issues have been a much more significant challenge to the accuracy of facial recognition technology over its 20+ year history of development. The December 2019 NIST Demographic Effects report provides a comprehensive answer to many of the public's most pressing questions about facial recognition accuracy and related concerns about bias. It found highest performing technologies had "undetectable" differences in performance across demographic groups, while most others performed much more consistently than had been widely reported in the media and a number of non-scientific tests.[3] While some commentary has focused on the very lowest-performing algorithms, it's important to point out that key public sector programs are already using the highest-performing technology tested – with accuracy rates well above 99% and undetectable false positive differences across demographics, even when tested against galleries of up to 12 million images.

We understand that there are legitimate concerns that use of facial recognition technology might negatively impact women and minorities. Industry is striving to provide technology that is as effective and accurate as possible across all types of uses, deployment settings and demographic characteristics in order to fully address these concerns. Biometric technologies like facial recognition increase the effectiveness of safety and security applications, ultimately helping to better protect people from harm. Any significant bias in technology performance makes it harder to achieve this goal.

On behalf of SIA and its members, we urge the City Council to reject this proposal its current form, and seek less extreme measures that address public concerns about facial recognition without putting public safety at risk by a blanket ban on all current and future uses of this critically important technology tool.

Please let us know if we can provide further information or assistance as you consider these important issues.

Sincerely,

Don Erickson
Chief Executive Officer
Security Industry Association

Staff Contact: Jake Parker, jparker@secuirtyindustry.org

CC: Members of the Boston City Council, Marty Walsh, Mayor, City of Boston

[2] https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software
[3] https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/