February 24, 2021

The Honorable Mark Conway
Chair, Public Safety and Government Operations Committee
Baltimore City Council
Du Burns Council Chamber, 4th floor, City Hall
Baltimore, MD 21202

Written Testimony of SIA in Opposition to Council Bill 21-0001 Banning the Use of Facial Recognition Technology

Dear Chairman Conway and Members of the Public Safety and Government Operations Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with the proposed ordinance, which would prohibit the use of facial recognition technology by city government as well as private entities in the city, including individuals and businesses. SIA is a nonprofit trade association representing companies that provide a broad range of security products and services in the U.S and throughout Maryland, including 27 companies headquartered in our state. Our members include many of the leading developers of facial recognition software as well as companies offering products that incorporate this technology into a wide variety of government, commercial and consumer products.

Support for Ensure Responsible, Ethical Use

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies provide both benefits and the potential for misuse, banning a specific technology is not a panacea for addressing concerns. Facial recognition technology is used in a wide variety of applications that have completely different implications. Addressing concerns about facial recognition can and should be accomplished through policies ensuring it is only used for appropriate purposes and in acceptable ways.[1]

Blanket Ban vs. Sensible Safeguards

A blanket ban would strip away the opportunity for policymakers to both limit potential uses of concern and preserve the benefits the technology can provide, both now and in the future. There are ways this can be done. We support the Baltimore Police Department's proposal to the council to replace the prohibition in the bill regarding law enforcement use, with safeguards that will help "prevent intentional misuse and to reduce the possibility that an innocent individual could suffer from negative consequences," including publishing use policies that establish key limitations and implementing new reporting requirements and regular audits of the use of the technology.

This approach would formalize many procedural safeguards governing law enforcement use while preserving the proven benefits to residents of Baltimore and the state, where it has been used for many years to enhance the speed and accuracy of identification processes needed to solve cases. There are many examples.[2] In 2018 it was used to help identify the gunman that killed five employees and critically injured two others at the Capital Gazette headquarters in Annapolis. In 2019 it was used to help identify bank robbery suspect and break up an organized crime ring in

[1] See SIA's recommendations - https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

[2] [2] https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/

Montgomery County. Just last year in Baltimore it was used to help identify the perpetrator of a brutal assault on public transit, which was confirmed by the victim. We know that using high-quality facial recognition technology, combined with trained human review, can identify individuals more accurately than most people can unassisted.[3] Banning all facial recognition technology would also eliminate an important tool for checking and mitigating human bias.

Bill Would Ban Proven Business Applications

Similarly, we would support sensible rules for use of the technology in the private sector. However, the term "face surveillance" as defined in the ordinance encompasses virtually any use of facial recognition for identification or identity verification purpose. This means nearly all private sector applications of facial recognition would be banned under the ordinance, including those with obvious benefits to the users and have nothing to do with surveillance, policing or civil liberties concerns. This will shutter the ability of Baltimore businesses to use advanced technologies in beneficial and ways.

In fact, most provide sector applications are opt-in, where there is already user consent or an existing requirement to verify one's identity. This includes allowing customers to prove their identities conveniently and securely for banking or other financial transactions, customized service in the hospitality and gaming industries, and for additional security measures at entertainment venues and other facilities.

Additionally, the technology is becoming increasingly important to COVID-19 mitigation protocols in business operations. For example, it is included in currently fielded technology that performs elevated body temperature screening and allow users to seamlessly provide vaccine validation, test results and other info needed to enter a workspace or perform other activities, while also providing a contact tracing information if they are exposed to the virus.

Businesses and individuals in Baltimore City would face criminal penalties through fines or imprisonment for uses in everyday business operations, even social media applications - an intervention in commerce, private property and the lives of individuals that demands a strong and thorough justification.

What the Science Really Says About Facial Recognition Accuracy

Additionally, you may have heard the oft-repeated claim in media reports about racial "bias" in the technology. What this really refers to is the performance of of the software in successfully comparing and matching photos of the same person. While it is true some versions of the technology have struggled to provide consistent performance across racial and other demographic factors, the claim that all facial recognition technology is less accurate across the board in matching photos of black and female subjects does not accurately reflect the current state of the science.

The National Institute of Standards and Technology (NIST), the leading scientific authority worldwide on the accuracy of facial recognition algorithms, found in its Demographic Effects report in 2019 that the leading facial recognition technologies it tested had "undetectable" differences[4] in accuracy across racial groups, after rigorous tests against millions of images. This would simply not be the case if demographic differences were "inherent" in the technology. These leading technologies are the same ones used in most of today's government and law enforcement applications, reaching the accuracy of fingerprint technology on many measurements, the gold standard for identification.

At the same time, lower performing algorithms among the nearly 200 that NIST tested did show measurable differences of several percentage points in performance across demographics – and this is an issue utmost importance to our

[3] https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-expertsperform-better-ai-partner
[4] https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/

industry which is continually addressed. It is critical to understand though, that most still had overall accuracy rates around 99% for all categories.

Widely misconstrued in media accounts is a 2018 report[5] where the claim is that it showed a 35% error rate for facial recognition on photos of black women. In fact, those researchers tested older "face gender classification technologies." Such software used to classify the race, gender, age, etc. of an unknown person in a photo – a technology that is not used for identification, or in law enforcement. Facial recognition, on the other hand, compares two or more images for similarities to help identify a specific person based on their unique facial features. By conflating these technologies and citing research that did not actually evaluate facial recognition accuracy at all, many media reports inaccurately assigned racial disparities[6] to facial recognition that really dealt with a different technology.

Americans Support Current Uses of Facial Recognition

Finally, leading independent polling firm Schoen Cooperman Research recently conducted a nationwide poll on Americans' views of facial recognition technology, commission by SIA.[7] The survey found 68% of Americans believe facial recognition can make society safer, 70% believe it is accurate in identifying people of all races and ethnicities and 66% of believe law enforcement's use of facial recognition is appropriate. 70% supported use by banks, and to improve workplace safety. The results are consistent with other polling that indicates little public support for banning or heavily restricting this important technology.

On behalf of SIA and its members, we share the goal of ensuing responsible use of advanced technologies and would support policies ensuring that facial recognition is only used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve the ordinance in its current form. We stand ready to provide any additional information or expertise needed as you consider these issues.

Sincerely,

Respectfully,

Jake Parker
Senior Director, Government Relations
Security Industry Association
Silver Spring, MD
jparker@securityindustry.org

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

CC: Members of the Public Safety and Government Operations Committee

[5] https://www.media.mit.edu/projects/gender-shades/overview/
[6] https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition
[7] https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/