



December 3, 2020

The Honorable Charlie Baker
Governor of the Commonwealth of Massachusetts
Massachusetts State House, 24 Beacon St.
Boston, MA 02133

Re: Urging reconsideration of the ban on public sector use of facial recognition technology included in the police reform measure, S. 2963, Section 26, Chapter 6, passed by the General Court

Dear Governor Baker:

The International Biometrics + Identity Association (IBIA), the leading voice for the biometrics and identity technology industry, appreciates this opportunity to present these comments on the police reform bill, S. 2963, Section 26, Chapter 6, that would ban government use of facial recognition technology in Massachusetts.

IBIA supports the transparent and lawful use of technologies to confirm and secure human identity in our physical and digital worlds. Our members include biometric technology researchers, developers, providers, and users around the world. Several of our most prominent members are based in Massachusetts, and many more provide products and services to public- and private-sector entities in the Commonwealth.

IBIA understands the need for criminal justice system reform. However, banning facial recognition technologies, along with the other remote technologies enumerated in Chapter 26, would harm, not help, reform efforts. According to NIST testing results and GAO reports, the accuracy of facial recognition algorithms and performance across demographic populations are highly accurate and facial recognition is now widely used and accepted throughout society.¹

Given the widespread and deep benefits of responsible use of facial recognition technologies, IBIA respectfully urges you to reconsider Section 26, Chapter 6, in S. 2963, the police reform bill that would ban government entities statewide from using virtually all uses of facial recognition technologies, identity technology vendors have improved the accuracy, commercial marketability, and versatility of facial recognition and other biometric modalities, and these technologies have become widely accepted throughout the ever-growing global information technology marketplace.² Top-performing facial recognition technologies are now highly accurate overall and across demographic groups.³

¹ See *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses* 8-12, 25-26, <https://www.gao.gov/assets/710/708045.pdf>.

² See *id.*; *FRVT Part 3: Demographic Effects (NISTIR 8280)* 8, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

³ See *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses* 4-7, <https://www.gao.gov/assets/710/708045.pdf>

Given the tremendous benefits that responsible use of facial recognition technologies can produce, IBIA respectfully urges you to reconsider the facial recognition ban in Section 26 of S. 2963.

- **The Definitions in Section 26, Chapter 6 are Overly Broad and Misleading**

Section 26 defines a ‘biometric surveillance system’ to include ‘facial recognition’. In effect, this definition conveys the impression that all uses of facial recognition constitute some form of ‘surveillance’. (The section also refers to ‘other remote biometrics’ but the focus of the legislation appears to be facial recognition.)

In addition, the definition of facial recognition includes, not only its long-standing use for identification and verification, but also to “capture information about an individual based on the physical characteristics of individual’s face, head, or body to infer emotion, associations, activities, or the location of the individual”.

Facial recognition and surveillance are entirely different processes and conflating them is inconsistent with settled longstanding government and academic research entities.

The cause for IBIA’s concern is the use of this overly expansive definitions will preclude an informed discussion on the public safety and security benefits of facial recognition technology to the detriment of the citizens of Massachusetts.

Based on this overly-expansive definition, the Section issues a statewide ban on virtually all facial recognition uses for verification or identification and also to infer emotion, associations, activities or location of an individual.

Facial recognition is only about the identification of a human face and the ability to match it to a single known facial image. Facial matching is only useful to match against a known gallery of quality facial images to those submitted to it for matching. There is no database of all faces so an unknown individual will still remain anonymous after a non- match. The reality is that a very large swath of the population is not on file anywhere in the US.

Surveillance, on the other hand, is the active real-time watching of people, places, and things. Merriam-Webster defines “surveillance” as “close watch kept over someone or something (as by a detective).” It can be done with recorded video and human review. Video surveillance cameras are in wide use today and capture entire scenes for later playback, if needed.

- Facial recognition is understood to be 1:1 verification and 1:N identification. They are different applications.
- 1:1 verification using facial recognition is normally a passive activity, where action is taken on-demand for various types of access -- secure borders, aviation security, building security
- 1:N use of facial recognition is used for post-event investigations to help law enforcement agencies and other agencies to identify identify crime victims; process forensic evidence; and generate investigative leads.
- Using facial recognition technology in conjunction with video surveillance camera footage post-event merely automates and improves the accuracy and efficiency of a process that humans are currently manually performing.

Conflating facial recognition with surveillance in the definitions will preclude an informed discussion about the benefits and risks of facial recognition technology.

- **Facial Recognition and Other Biometric Technologies Play an Important, Beneficial Role in Our Lives**

As recent reports from the Government Accountability Office⁴ and the Congressional Research Service⁵ have demonstrated, facial recognition technologies help law enforcement agencies and other public-sector entities improve border security, aviation safety, and building security; identify crime victims; process forensic evidence; and generate investigative leads. After detailing the multitude of benefits and analyzing the risks that facial recognition technologies can create, neither of these reports recommends banning facial recognition technologies.

We appreciate public concerns about the misuse of facial recognition technologies through mass surveillance, and we unequivocally oppose the misuse of facial recognition technologies in these clearly harmful ways. However, all facial recognition technologies do not constitute surveillance as the definition in this legislation suggests,⁶ which is why we advocate for a use-case-specific, risk-based approach to facial recognition legislation.

Our members strongly support efforts to build public trust in facial recognition technologies, but we do not believe that banning facial recognition will build public trust.

On the contrary, facial recognition bans will only serve to further strain relationships and erode trust between government agencies, the communities they serve, and the technology providers that want to help government agencies effectively serve all members of their diverse communities.

Banning government agencies from using innovative technologies will result in continued reliance on existing techniques that are considerably less effective and leave equal or greater room for human bias (such as the bias that often contributes to inaccurate eyewitness identifications) to produce unjust outcomes. The inaccuracy of identifications in our existing systems is a significant factor contributing to the lack of trust between law enforcement agencies and the communities they serve.

The alternative is to incorporate new and better technologies that help improve the accuracy of identifications; develop transparent and secure processes and standards to govern their uses; educate people about how the technologies work, their benefits, and the applicable framework to protect the community and build an atmosphere of trust.

Facial recognition bans will deprive communities of tools that can help promote accountability, safety, security, efficiency, and privacy.

The ban on public-sector use of facial recognition would harmfully limit law enforcement officers' ability to:

- More accurately identify suspects, reduce human error, and lessen the impact that human biases have in perpetuating criminal justice system inequities;
- Eliminate innocent people as potential suspects;

⁴ See *id.*

⁵ <https://www.gao.gov/products/GAO-20-568>

⁶ <https://crsreports.congress.gov/product/pdf/R/R46586>

- Generate investigative leads in cold cases;
- Identify disoriented individuals, including those with amnesia, dementia, and Alzheimer’s disease;
- Identify unconscious or deceased crime victims;
- Identify human trafficking victims;
- Detect the use of stolen or fraudulent identity documents; and
- Quickly identify and apprehend individuals who may be perpetrating ongoing crimes, such as kidnappings, mass shootings, and bombings.

The ban would also harmfully prohibit government entities from using facial recognition technologies to:

- Improve building security by identifying authorized entrants and keeping unauthorized entrants out;
- Improving data privacy and data security by identifying individuals seeking to access secure physical and digital government records;
- Alerting security officers to the presence of individuals who have previously committed crimes on government property or have threatened violence against government officials; and
- Promote health and safety by facilitating efficient, contactless access control (and contact tracing for those who opt-in) in government facilities, such as hospitals and other healthcare facilities.

In recognition of these negative impacts of banning facial recognition technologies and denying the public the benefits that these technologies can produce, other progressive jurisdictions that pride themselves on fostering innovation have established requirements that public-sector entities using facial recognition technologies must satisfy, rather than outright banning the technologies.⁷

No other U.S. state has passed a statewide ban on public-sector use of facial recognition technologies, and we urge Massachusetts to avoid becoming the first jurisdiction to do so. Rather, we encourage Massachusetts to act in accordance with its longstanding view that technological progress spurs social progress, and we ask Massachusetts to maintain its supportive approach to encouraging scientific research and technological development.

- **An Alternative Approach to Facial Recognition Legislation Can Mitigate Risks Without Unduly Limiting Benefits**

Instead of banning or unduly restricting law enforcement and other public-sector uses of facial recognition, legislative efforts should adopt a more nuanced, risk-based approach. Such legislation should aim to ensure that law enforcement agencies and other public-sector entities procure facial recognition technologies that perform accurately overall and across demographic groups through a transparent process that is subject to oversight. Additionally, legislation should clearly convey that existing Constitutional protections apply to public-sector uses of facial recognition.

⁷ As GAO explains, facial recognition technologies perform a variety of different functions, including detection, verification, and identification, in conjunction with both still photos and video footage. See *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses 4-7*, <https://www.gao.gov/assets/710/708045.pdf>. Concerns about using facial recognition technologies to facilitate mass surveillance largely revolve around performing identification on real-time video footage without people’s knowledge or consent.

IBIA is not alone in advocating for this approach. Along with several other industry groups and companies that have conveyed their opposition to the police reform bill's facial recognition provision, we understand that Attorney General Healey has raised specific concerns about the misconceptions surrounding facial recognition and the potential unintended negative consequences of a broad public-sector ban.

Before banning or restricting facial recognition technologies, we respectfully urge you to fully consider all the facts, including those which media articles criticizing the technologies frequently omit.

IBIA believes a special commission or task force, like the law enforcement body camera task force (Section 104) and the special legislative commission (Section 105) that the bill would establish, can contribute to a careful consideration of facial recognition technologies and their risks, benefits, capabilities, and limitations. However, to be effective, such a task force or commission must reflect and consider perspectives from the full array of relevant stakeholders. To ensure that the task force's and special legislative commission's studies and recommendations are as robust and informed as possible, we recommend including more biometric technology experts from both the developer and end user communities.

- **Conclusion**

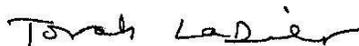
IBIA respectfully urges you to avoid taking the drastic, unprecedented step of broadly banning public-sector use of facial recognition technologies before learning more about the different functional applications and use-cases.

Instead, IBIA respectfully asks the General Court to adopt a more use-case-specific, risk-based approach to developing procurement and use requirements that mitigate the concerns these technologies can pose while allowing Massachusetts residents to enjoy the many benefits that these technologies can produce.

IBIA is committed to working with policymakers and other stakeholders to ensure that facial recognition technologies are used responsibly by law enforcement as a tool to help solve crimes, keep our communities safe, and mitigate concerns about the technology. We would be happy to serve as a resource to you and other Massachusetts policymakers seeking to learn more about the transparent and secure use of facial recognition technologies.

Please do not hesitate to let us know how we can be of further service.

Sincerely,



Tovah LaDier
Executive Director