International Biometrics+Identity Association

Comments on Section 25 of MA H. 4860 on Facial Recognition Ban

Overview

The International Biometrics + Identity Association (IBIA), the leading voice for the biometrics and identity technology industry, appreciates the opportunity to present these comments on H. 4860, Section 25, that bans the use of facial recognition technology in all MA government agencies.

IBIA respectfully urges the reconsideration of Section 25 until there has been an opportunity to fully consider the facts about facial recognition technology and its important benefits. This is particularly important given that the discussions on the topic tend to take place in an environment charged by sensationalism and fearmongering.

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

This Bill's Basic Premise is an Incorrect and Misleading Definition of Facial Recognition

The bill defines a 'biometric surveillance system' to include 'facial recognition'. It conflates two (2) entirely different processes. Facial recognition and surveillance are not the same. Conflating them is a misconception based on hypothetical statements, not facts.

- 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.
- Facial recognition is usually understood to be 1:1 verification and 1:N identification, which are significantly different applications with very different privacy concerns. Facial recognition is normally a passive activity, where action is taken on-demand (1:1) for various types of access, or post-event (1:N) for investigation.
- Video surveillance cameras are in wide use today and capture entire scenes for later playback, if needed.

- Surveillance is the active watching of people, places, and things. It can be done with recorded video and human review, or more recently technology has evolved so that video analytics can look for watch listed persons in recorded material or even real-time. A really big watchlist would be 100,000 persons.
- Using facial recognition technology in conjunction with video surveillance camera footage merely automates and improves the accuracy and efficiency of a process that humans are currently manually performing.

Inference of emotion, association, activities, criminal inclinations is **NOT** facial recognition. So far, beyond pseudo-science, it does not have a discipline name. It does not belong in this analysis.

Biometrics Play an Important Role in Our Lives

In the past few years, biometrics and identity industries have made great strides in improving the performance and utility of their products. The uses of the technologies have expanded dramatically from niche law enforcement and security tools to become globally accepted and established elements of the ever-growing information technology marketplace.

Consider that the process of identifying humans based on their faces is as old as the human race itself. Facial recognition technology does not introduce new identity paradigms or capabilities; it merely adds to the efficiency, accuracy, and reliability of computers to enhance our human recognition.

Section 25 Does Not Provide a Rationale for the Overly Broad Statewide Ban

Based on its faulty definition of facial recognition, Section 25 would enact a statewide ban on most government uses of facial recognition.

There is no reason provided for such sweeping action.

Section 25 Ignores the Important Benefits of Facial Recognition to Public Safety and Security

Automated facial recognition can do things that humans cannot do. Machines can memorize millions of faces, humans only thousands; this enables machines to do things unaided that humans cannot.

This proposed blanket ban on facial recognition (as currently defined in H.4860) will preclude its use in forensic analysis, not only severely limiting the capability of law enforcement officials to solve crimes, but also to

- Identify disoriented (amnesia, dementia, Alzheimer's, etc.) adults.
- Identify fraudulent use of stolen identity documents.

- Make highly accurate cross-racial identifications, with top performing commercial algorithms.

Facial recognition is also critical in real time in cases of mass shootings, bombings, and other disasters. The technology has improved by orders of magnitude and facial recognition now is a crucial element in counterterrorism and law enforcement around the country and the world. Instead of banning or seriously restricting law enforcement and other public-sector uses of facial recognition, legislative efforts should aim to ensure that existing Constitutional and civil liberties protections apply to public-sector uses of facial recognition.

Section 25 Does Not Acknowledge the Undisputed Superiority of Facial Recognition Compared to Human Recognition

- Skilled humans are about 80% effective recognizing/identifying unfamiliar persons than automated facial recognition.[1]
- The top algorithms are 99% accurate across all demographic groups, scale no collection of humans can match.[2]
- The top 40 algorithms outperform the median of all human groups, including forensic face examiners.[3]
- The top two (2) commercial algorithms exhibit no performance differentials across demographic groups.[4]

In many circumstances people are, and must be, identified by their faces. It makes no sense to exclude the use of technology for activities humans are widely known not to be good at. The Innocence Project has found that 70% of convictions secured on the basis of eyewitness testimony were reversed due to faulty eyewitness testimony.

Special Commission Structure Does Not Lend Itself to a Serious Impartial Analysis of the Issues

A special Commission is charged with eight objectives:

- Examine and evaluate the facial recognition system operated by the registry of motor vehicles and provide recommendations for regular independent bias testing.

[1] White D, Kemp RI, Jenkins R, Matheson M, Burton AM (2014) Passport Officers' Errors in Face Matching. PLoS ONE 9(8): e103510. https://doi.org/10.1371/journal.pone.0103510

[2] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280, (pp. 1–79). doi: 10.6028/nist.ir.8280 Re

[3] Op. cit.

[4] Op. cit.

- Propose standards to ensure accuracy and equity of the system based on age, race, gender and religion.
- Examine access to the facial recognition system and the management of information derived from it, including, but not limited to, data retention, data sharing and audit trails.
- Identify which federal agencies, if any, have access to databases maintained by the commonwealth that catalogue images of faces and the authorization for, and terms of, such access.
- Evaluate the requirement for a warrant by law enforcement agencies to perform facial recognition searches, including, but not limited to, enhanced requirements to perform a search similar to those set forth in section 99 of chapter 272 of the General Laws.
- Provide recommendations for due process protections of criminal defendants when facial recognition technology is used in any part of an investigation.
- Provide recommendations to ensure privacy for the public.
- Provide recommendations for adequate training and oversight on the use of facial recognition technology.

The membership largely includes government officials, academics with privacy expertise, and privacy organizations.

Noticeably excluded are the technology developers, academic researchers, and the major users. It makes little sense to exclude from the Commission many of the individuals who have a strong technical understanding the technology involved. These entities have the first-hand information on how current systems function, what is feasible, how to protect and share data, and how to ensure compliance with limitations imposed on the use of facial recognition, without unintended consequences.

Conclusion

IBIA respectfully urges the MA House to reject the sweeping ban on facial recognition use by all government agencies.

- Section 25 is based on an incorrect and misleading definition of facial recognition that suggests it is misused for surveillance purposes.
- Biometrics play an important role in our lives.
- Section 25 does not provide a rationale for the overly broad statewide ban.
- Section 25 ignores the important benefits of facial recognition to public safety and security.
- Section 25 does not acknowledge the undisputed superiority of facial recognition compared to human recognition.
- Special commission structure does not lend itself to a serious impartial analysis of the issues.