



International  
**Biometrics+Identity**  
Association

# **Comments from IBIA on MA S. 1385 and MA H.1538: legislation proposing to place a moratorium on facial recognition technology**



November 4, 2019

The Honorable James Eldridge  
24 Beacon St.  
Room 511-C  
Boston, MA 02133

The Honorable Claire D. Cronin  
24 Beacon St.  
Room 511-C  
Boston, MA 02133

The Honorable Cynthia Creem  
24 Beacon St  
Room 312-A  
Boston, MA, 02133

The Honorable David M. Rogers  
24 Beacon St  
Room 544  
Boston, MA, 02133

Dear Senator Eldridge, Senator Creem, Representative Cronin, and Representative Rogers:

These comments respond to legislation proposing to place a moratorium on facial recognition technology ([MA S. 1385](#) and [MA H.1538](#)). They are submitted by the International Biometrics + Identity Association (IBIA), the leading voice for the biometrics and identity technology industry.

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.

### **IBIA Position on Proposed Biometrics Moratorium Legislation**

IBIA respectfully urges that the Judiciary Committee refrain from passing the bills until there has been an opportunity to fully consider the facts about the 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 is confident that thoughtful consideration will illuminate the manifold ways in which the use of biometric technologies such as facial recognition need not pose a threat, but rather are essential to ensuring public safety, now and in the future.

## Surveillance is the Root Concern among Citizens, Not Technology

IBIA believes that the root concern among privacy advocates and the general public is not with biometrics technology itself—which is used every day in some form around the globe by billions of people—but with the act of government surveillance. While technologies offer an easy target, biometrics is merely a software technology; a form of mathematics used to assess the similarity of biometric data such as facial images. In and of itself, biometrics technology does not pose a threat of any kind to anyone.

We therefore strongly recommend that legislative efforts place appropriate focus on the root sources of public concern; that they avoid casting false blame on legitimate and useful technologies that deliver such important benefits for a broad variety of applications for so many people every day.

For example, instead of an outright ban on technology, legislators might consider:

- 1) the conditions under which surveillance should and should not be permitted, and
- 2) the ways in which identity data captured by the DMV for the purpose of printing driver's licenses may or may not be used or shared.

## 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 use of facial images for identity is as old as the human race itself. Biometrics 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 capabilities towards more convenient, trusted interactions between individuals.

The public recognizes the value of biometrics and facial recognition for law enforcement and safety. A recent [poll](#) by Net Choice of 600 Massachusetts residents conducted by Savanta Analytics shows a majority of Bay Staters do not support the current legislative proposals. The poll findings are as follows:

- 66% say law enforcement should not be precluded from using new technologies, such as facial recognition, to fight crime
- 64% say facial recognition technology has the potential to enhance safety
- 46% say government should not strictly limit the use of facial recognition technology if it comes at the expense of the public's safety
- 15% **only** want to limit law enforcement's use of the technology, even if it comes at the expense of the public's safety

## **The Broad Scope of the Bills Poses Serious Risks to Public Safety**

The pending bills would enact a statewide ban on government uses of facial recognition, making Massachusetts home to the first statewide ban in the country. There is a strong risk that legislation misrepresenting the technology as a threat will have effects that are much farther-reaching and unpredictable than intended. We fear that such efforts will ultimately distract the public from legitimate privacy concerns with surveillance.

The bill provides, “it shall be unlawful for the Commonwealth of Massachusetts or any Massachusetts government official to acquire, possess, access, or use any biometric surveillance system, or acquire, possess, access, or use information derived from a biometric surveillance system.”

The problem is that a “biometric surveillance system” is then defined “as any computer software that performs face recognition.” This terminology reflects incorrect rhetoric that conflates biometrics with surveillance. The term, “biometric surveillance system” is not one that is used in security, aviation, law enforcement or public safety. The definition used in the bill is vague and broad; it covers all devices that perform face recognition – presumably including ubiquitous handheld mobile phones, tablets and other devices that are inextricable from daily life in the 21<sup>st</sup> century. Presumably, the bill would also apply to Massachusetts government officials who use mobile devices. A ban on all uses of an important and beneficial technology that is widely used in commercial mobile phone devices and computers.

This proposed blanket ban on facial recognition will also preclude its use in forensic analysis, severely limiting the capability of law enforcement officials to solve crimes, identify missing and abused children, and apprehend human traffickers, to name just a few of the vital missions that are enhanced by the use of facial recognition.

Facial recognition is also critical in real time in cases of mass shootings, bombings, and other disasters. In the case of the Boston Bomber, facial recognition was not at its current level of sophistication. The FBI and other law enforcement spent countless hours reviewing photos and videos before the two brothers were determined to be suspects and in-depth investigation could begin. Since the Boston Marathon bombing, 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.

## **The Bills Are Based on Erroneous, Sensational Claims Intended to Stoke Fears but Uninformed by Facts**

The Preambles contain justifications that are factually inaccurate, misleading, and likely to result in significant detrimental consequences for Massachusetts and its residents. It perpetuates debunked, inaccurate, and misleading rhetoric. It appears the Preamble was not drafted with input from experts from industry, user communities, the Federal Government, NIST, or international standards bodies. These stakeholders can provide valuable insights about

the technology, how it is actually used, and the privacy-enhancing potential of biometrics. Their input should be considered essential in crafting sensible policy that avoids influence from false or inflammatory rhetoric designed to stoke irrational fear of a misunderstood technology.

### False Statement #1: Facial Recognition is Inaccurate Across Varied Populations

*The truth: Facial recognition is extremely accurate and rapidly becoming more so as demonstrated by exhaustive tests by NIST.*

The Preamble states that, "... the technology has a history of being far less accurate in identifying the faces of women, young people, and dark-skinned people than lighter skinned people and that such inaccuracies lead to harmful 'false positive' identifications." This statement is false and is not informed by established testing and research of the technology.

Nearly every story that buys into this portrayal of facial recognition cites as this so-called "history" references a single 2012 study by Brendan Klare et. al., *Face Recognition Performance: Role of Demographic Information*.<sup>1</sup> The study's principal author has recently made clear that paper is not a basis for the claims of bias others have made.<sup>2</sup> Even if the claims were accurate seven (7) ago when it was written, the rapid pace of technological advancement underscores the paper's inherent weakness as a piece of documentary evidence. The latest 2019 Department of Commerce National Institute of Standards and Technology (NIST) reports and several academic studies demonstrate the obsolescence of Klare's paper, as he himself has said.

The top 100 performing 1: 1 algorithms reported by NIST in the October 2019 *Ongoing Face Recognition Vendor Test (FRVT)*, identify dark-skinned people more accurately than white people.<sup>3</sup> The scientific and evidence-based NIST studies, not the outdated assertions of special interest privacy groups with a political agenda, are the internationally recognized gold standard on the subject. The NIST results are updated regularly. NIST posts the studies and results on the Internet and the studies are freely available to the public. IBIA encourages legislators to review the latest NIST reports on the state of the technology and seek the expert input of these and other researchers. Consulting the scientific community will provide a current and accurate understanding of the state of the technology.

### False Statement #2: Facial Recognition is Analogous to a National ID Requirement

*The truth: There is no equivalency between facial recognition technology and a compulsory national identity program.*

The Preamble asserts that facial recognition is a danger to privacy and civil liberties because it is, "the functional equivalent of requiring every person to carry and display a personal photo identification at all times."

This type of rhetoric again intends to stoke fear but simply has no basis in reality. At best, it displays a basic lack of understanding about the technology and how it is used. For example,

facial recognition technology does not identify persons not already enrolled in a law enforcement database as a result of arrest or conviction.

It also incorrectly and irresponsibly presumes the technology is on hand to identify vast numbers of people and track their movements in real time. While these concepts are a staple of television drama, they are far from reality.

### False Statement #3: Facial Recognition Benefits Are Speculative

*The truth: Facial recognition and other biometric technologies has been proven essential to law enforcement, border security, and public safety.*

The Preamble states that the “Benefits of Facial Recognition are few and speculative”. There is no evidence provided to support this assertion. Here is a partial list of the many positive benefits of facial recognition, which humans alone cannot do quickly, without the help of technology:

- Identify disoriented (amnesia, dementia, Alzheimer’s, etc.) adults
- Flag likely driver license application fraud for human review
- Identify fraudulent use of stolen identity documents
- Make highly accurate cross-racial identifications
- Enhance aviation security and facilitate passenger travel by allowing individuals to move seamlessly through airports without having to show agents personally identifiable information on government-issued documents.

### **Concluding Remarks**

Bills banning use of facial recognition should be tabled and legislators should work on developing constructive and workable legislation, based on real facts and real threats.

The industry stands ready to meet and work with you and your members at any time. IBIA is currently engaged in developing constructive solutions to ensure that facial recognition is used appropriately and beneficially. We would be pleased to discuss our efforts with you, answer your questions and provide tailored seminars and tutorials for you and your colleagues.

We also encourage you to seek further input from experts who are using the technology for public benefit, as well as those conducting research and standards development. Industry welcomes opportunities to inform policymaking that delivers the benefits of biometrics to Massachusetts residents while protecting their privacy and civil liberties. In the case of facial recognition, these concepts are not mutually exclusive.

IBIA appreciates this opportunity to submit written comments for the record and looks forward to working with you. If you have questions, please do not hesitate to contact us.


In the meantime, attached are materials that IBIA has drafted on these issues that provide

additional details:

[Understanding the Performance of Facial Recognition Algorithms](#)  
[Open Letter to Congress on Facial Recognition](#)  
[Principles for Biometric Data Security and Privacy](#)

Sincerely,

Tovah LaDier



IBIA Executive Director

**About IBIA:** The IBIA is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. Visit us at [\*\*www.ibia.org\*\*](http://www.ibia.org).

## Endnotes

---

<sup>1</sup> Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on Information Forensics and Security*, 1-14.  
<http://openbiometrics.org/publications/klare2012demographics.pdf>

<sup>2</sup> Klare, B. (2019, September 19).  
<https://blog.rankone.io/2019/09/12/race-and-face-recognition-accuracy-common-misconceptions/>

<sup>3</sup> Grother, P., Ngan, M., & Hanaoka, K. (2019). *Ongoing Face Recognition Vendor Test (Frvt)*. *Ongoing Face Recognition Vendor Test (FRVT)* (16th ed., pp. 1–646). NIST .  
[https://www.nist.gov/sites/default/files/documents/2019/10/16/frvt\\_report\\_2019\\_10\\_16.pdf](https://www.nist.gov/sites/default/files/documents/2019/10/16/frvt_report_2019_10_16.pdf)