International Biometrics+Identity Association

May 29, 2020

RE: IBIA Comments on Draft Bill To Establish a Moratorium on *"New Uses of Facial Recognition Technology by Agencies"*

Thank you for giving IBIA the opportunity to comment on your draft bill "To Establish a Moratorium on New Uses of Facial Recognition Technology by Agencies".

IBIA supports the Committee's goals of transparency, accountability and standards for the use of all biometrics, including facial recognition. IBIA, however, believes that a moratorium on the use of facial recognition, even if limited to new federal government uses of facial recognition, is not in the best interests of the country and will have adverse consequences for the public, business, and the country. For these reasons, IBIA cannot support this bill as drafted.

IBIA believes there are other options, short of a facial recognition moratorium and proposed advisory committee this bill proposes, to develop principles for the transparent, secure, and trustworthy use of facial recognition, including, addressing specific problems that may exist rather than a wholesale moratorium on the use of facial recognition and, a mechanism to facilitate the development of principles for the appropriate use of facial recognition.

IBIA looks forward to working with the Committee as it continues its deliberations.

Comments

The enumerated Findings, which outline the rationale for the draft bill, do not include information critical in considering facial recognition legislation and are not entirely clear on several technical points.

- Latest NIST test results that show that performance of top performing algorithms have undetectable differences among demographic groups.[1]
- Benefits of facial recognition.
- Serious risks of an open-ended moratorium on facial recognition to public safety and national security.

[1] 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

- Government processes that ensure transparency and accountability of facial recognition use already exist.
- Although biometrics are not 'secret', they are not more vulnerable than passwords or social security numbers.
- Facial recognition is not synonymous with surveillance.

NIST Test Results: The test results showed wide variations in algorithm performance with respect to demographic differentials, and NIST explicitly states that it is not accurate to draw generalizations about algorithm performance. Some perform very well; others do not. The low performing algorithms show significant performance differences among demographic groups and are not attractive products to government or industry customers.

The results demonstrate that the most accurate **high-performing identification algorithms** (a one-to-many search in which the technology uses an image to search a database of images to find potential matches) display virtually 'undetectable' differences among demographic groups, greater accuracy than humans could ever achieve.[2]

The most accurate **high-performing verification algorithms** (a one-one verification search where 2 images are compared to determine similarities of the faces) display both low false positives and false negatives; more than 50 tested algorithms have false non-match rates (misses) less than three per thousand,[3] and false match rates (erroneous matches) less than one per hundred thousand,[4] again, greater accuracy than humans could ever achieve.

This latest report lists five (5) algorithms with an accuracy rate of 99.9%.[5] Other high-performing algorithms are in the 98-99% accuracy range.

Automated facial recognition is indisputably more accurate than current human recognition only systems. Measured accuracy of human visual passport inspection is notoriously low, determined by some to be in the range of 80% or less (for example, Passport Officers' Errors in Face Matching).[6]

---

[2] Op. cit. (pp. 3, 8)

[3] Op. cit. (pp. 54, 58)

[4] Op. cit. (pp. 56, 57)

[5] "Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification," Grother P., Ngan M., and Hanoka K., 2020/01/22, Pp 26-29

[6] 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

1325 G Street NW, Suite 554, Washington, DC 20005 **O: 202.888.0456 I W: IBIA.ORG**

The top performing algorithms outperform mean performance of all human groups including skilled forensic face examiners. Algorithm performance for the high performers, across the board, is more than 20 times better than skilled professional examiners.[7]

Benefits of facial recognition: Facial recognition has been proven essential to law enforcement, border security, and public safety and the automated facial recognition is also indisputably more accurate than current human recognition only systems.

This is a partial list of the many positive benefits of facial recognition, which humans alone cannot do quickly, without the help of technology:

- Identify missing children who do not know their names
- Identify exploited children in dark web pornography.
- Identify disoriented (amnesia, dementia, Alzheimer's, etc.) adults.
- Identify unconscious individuals who lack identification and need emergency medical care.
- 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.

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.

Any moratorium, even a moratorium limited to new uses of facial recognition technology, poses substantial risks to law enforcement, border security, and public safety where it has proven essential: For many critical public safety activities, it is not acceptable to limit performance to human capability, or alternatively to delay the use of and the implementation of upgrades and improvements for an undefined period of time.

---

[7] Private communication with James Loudermilk, Senior Director, National Security Solutions, an IDEMIA company and IBIA member organization, who did the analysis in an as yet unpublished paper.

1325 G Street NW, Suite 554, Washington, DC 20005 **O: 202.888.0456 I W: IBIA.ORG**

The covid-19 pandemic is a case in point. For health reasons, the focus on biometrics has shifted to the use of touchless biometrics. As drafted, the moratorium could preclude government agencies from upgrading existing technology for health reasons because they may require new vendors and totally new systems, even for the use of contactless biometrics.

No one forecast of the pandemic reveals a definite path forward so we have to preserve our ability to respond with the most cutting-edge technologies, and facial recognition with thermal sensing could facilitate safe access control as the economy opens. However, an open-ended moratorium on facial recognition could preclude agencies from using this important technology.

Government procedures already exist to ensure transparency and accountability: Numerous processes exist to ensure transparency and accountability with respect to facial recognition, such as privacy impact assessments and system of record notices. The contemplated reviews for the proposed advisory committee have already been done in full public view. All those interested in participating can do so for free and can also review regular reports that are already made available to the public.

The capabilities of the Departments of Justice, Homeland Security, and Defense are elements of large biometrics programs arising from research and development efforts extending over decades and multibillion-dollar procurements with broad national input and multiple Congressional hearings.

These programs have regularly briefed the Congressional Oversight Committees and during the multi-year developments underwent annual appropriations consideration.

As an example, the DOJ facial recognition technology requirements were developed with broad national input following hundreds of stakeholder group briefings prior to development; reviewed at least twice annually by the FBI Advisory Policy Board, a FACA Committee that is open to the public; and continues to perform that function during operation. The GAO has conducted reviews of the technology and there have been multiple oversight hearings. Much the same can be said for DOD and DHS.

Although biometrics are not 'secret', they are not more vulnerable than passwords or social security numbers: Biometrics are indeed not 'secret'. However, secret does not equal 'protection' and publicly revealed does not mean 'vulnerable.' The lack of secrecy does not make biometric systems less effective. It is in fact quite difficult to fool biometric systems.

The biometric data becomes important when it is associated with the sensitive biographic information of the individual, the prize because it can be used in many problematic ways. For this reason, it is highly important to separate the biometric and biographic databases and apply proper security measures, such as

1325 G Street NW, Suite 554, Washington, DC 20005 **O: 202.888.0456 I W: IBIA.ORG**

encryption, access controls, timely security patches, and liveness detection and anti-spoofing measures to ensure that facial recognition systems can detect spoofing attempts and identify individuals wearing face masks. Technology providers understand the potential risks associated with biometric data breaches and the need to implement robust data privacy and security features.

The real question is whether biometrics or usernames and passwords afford better protection. It is well-known that usernames and passwords provide limited protection and such compromises are frequently reported. On the other hand, the use of biometrics is expanding rapidly in all facets of our lives and no widespread problems have been reported.

Facial recognition is not synonymous with surveillance: This is a misconception based on hypothetical statements, not facts. Video surveillance cameras are in wide use today and capture entire scenes for later playback if needed. Facial recognition, on the other hand, 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.

There are no surveillance systems based on facial recognition. The cost of extending facial recognition to general surveillance would require a substantial appropriation action. No agency has sufficient discretionary funds to initiate such an effort, which means that Congressional authorization and appropriations, as well as OMB approval, would be required to set up a facial recognition surveillance system.

Conclusion

IBIA supports oversight and continued expansion of NIST testing and other efforts to strengthen NIST's role as the international gold standard for testing facial recognition and other biometric technologies. It is in society's best interest to develop a principle-driven, use-case-specific governance framework that both (1) carefully tailors restrictions to address specific risks that facial recognition technologies may pose in specific settings and (2) continues to support current and future beneficial uses of facial recognition technologies.

A facial recognition moratorium would do more harm than good. The US could lose its global leadership role in a highly critical national security technology; US companies could lose global business successes to competitors; and without a vibrant US industry, NIST's global leadership role in testing could be diminished.

1325 G Street NW, Suite 554, Washington, DC 20005 **O: 202.888.0456 I W: IBIA.ORG**

Again, thank you for inviting IBIA to provide input to the Committee's draft bill. Please let us know If you have questions or would like additional information

IBIA looks forward to working with the Committee.

Sincerely

Tovah LaDier

Tovah LaDier
Executive Director
IBIA

1325 G Street NW, Suite 554, Washington, DC 20005 **O: 202.888.0456 I W: IBIA.ORG**